Smart Mobs, Market Rebels, and Anonymous: Civil Disobedience in the 21st Century

J

Rutgers University
Abstract

John Rawls (1971) defines civil disobedience as a public, non-violent act and conscientious breach of law undertaken with the aim of bringing about a change in laws or government policies. On this account, the persons who practice civil disobedience are willing to accept the legal consequences of their actions. Traditionally, civil disobedience has operated in the physical world by breaking segregation laws, shutting down streets, and protesting in parks past their closing hours. Now, however, it has found a new platform by making its presence felt in virtual networks around the world. The Internet group Anonymous is one entity participating in the successful disruption of virtual spaces. This paper will focus on their concerted civil disobedience efforts on public and private entities, how direct action is mobilized, and the implications such actions have.
Welcome, Anonymous

On January 20, 2001, President Estrada of the Philippines became the first head of state in history to lose power to a smart mob. Over four days, more than a million citizens arrived causing the Estrada regime to fall and the legend of “Generation Text” was born (Rheingold, 2002). Nine years later, other heads of state from the Middle East joined Estrada’s fate during the Arab Spring at the hands of smart mobs.

The Arab Spring began in December 2010 with the Tunisian Revolution that ousted President Ben Ali. Uprisings in Egypt, Syria, Libya, Bahrain, Tunisia, and others commenced which led to Egypt’s Hosni Mubarak’s resignation and Libya’s Muammar Gaddafi’s execution. While the demonstrators exhibited courageous fortitude and resilience in the face of teargas, automatic weapons, and the possibility of torture and execution, network infrastructures and online civil disobedience helped support their efforts. Many individuals provided tech support, offering proxies as well as anonymizing software. Then, there was the role of the Internet group, Anonymous.

Although some describe their culture as vile and crude, Anonymous use their collective power to protest in virtual spaces against targeted public and private entities that engage in unethical practices ranging from censorship to corporate fraud. While they are noted for their Distributed Denial of Service (DDoS) attacks on the Church of Scientology, they were hurled into the limelight after successfully performing a DDoS attack on MasterCard.

The Third Era

Anonymous has transformed since its early days. At one time, they existed solely as a forum for pranks and humor. This era known by anons as *chan Anonymous, was conceived and embraced by users in the 4chan /b/, 7chan /b/, and other forums. Then, came the division
and arguments during their second era, Chanology Anonymous. This era was recognized as the civil war within Anonymous where some realized they could collectively organize politically while others had no such interest. The turning point, however, were the 2009 Tunisian protests (The Evolution of Anonymous, 2011).

Recognizing Internet censorship was taking place in Tunisia, Anonymous created a variety of manifestos outlining how to use encryption software as well as producing artistic videos for support and inspiration. By providing a variety of virtual artifacts for demonstrators, their *channer forums were DDoS’ed. Given this action and coupled with the solidarity surrounding Anonymous, they moved forward creating a new arm directed at political action (The Evolution of Anonymous, 2011). This third era is known as AntiSec Anonymous and landmarked by their participation in their DDoS attack against MasterCard and their HBGary hack¹.

On December 7, 2010, Visa and MasterCard began blocking donations to WikiLeaks (WikiLeaks, 2011). In turn, Anonymous DDoS’ed MasterCard by coordinating their efforts on an Internet Relay Chat channel. According to NYU professor Gabriella Coleman, one IRC channel had 7,000 confirmed users participating in the attack (Coleman, 2011). The large scale effort effectively shut down MasterCard preventing customers from accessing their website and were greeted instead with the following message:

---

¹ The definition of hacking has dramatically changed. For simplicity, hacking will be used in this paper to describe the breaking into and extraction of information from computing systems. Also, the media narrative and public perception on the hacker ethic are similar to the views on civil disobedience. While some actions are found as unlawful or immoral, others discern such acts as justified.
While many had viewed Anonymous as an immature group, their attack on MasterCard demonstrated their strength. It captured the eyes of the public and information security professionals, especially when they moved on to information security agencies.

**The HBGary fiasco**

A culture shift had taken place within Anonymous post Chanology. Despite providing network solutions and documentation for the Tunisian and Egyptian people, many anons were readjusting to the culture shock they were experiencing. “Where are the lulz?” asked many members (Coleman, 2011). The answer to that question appeared when HBGary, a firm specializing in computer security and web surveillance, was hacked in retaliation to a proclamation made by CEO Aaron Barr.

In an interview with Forbes, Barr said he had used a variety of social media techniques to track down leaders within Anonymous and threatened to release their names as well as their home addresses (ars technica, 2011). Anonymous responded by hacking his Twitter feed, his company website, and releasing internal company emails. Amongst the trove was a PowerPoint presentation entitled, “The WikiLeaks Threat” which outlined ways to undermine WikiLeaks and
“put pressure” on professionals who support the whistle-blowing website. Two outspoken and influential targets in HBGary’s sights were Tor developer Jacob Appelbaum and Constitutional lawyer and Salon journalist Glenn Greenwald. The following slide presents the company’s reasoning for targeting Glenn Greenwald.

This, of course, made matters worse for HB Gary, their partners, and Aaron Barr who eventually resigned. Anonymous had finally found the lulz and revival some of its members sought.

No holds barred, hash tag haven, and how Bruce Schneier negates media arguments

While continuing to provide support for demonstrators in the Middle East by jamming government websites, Anonymous was also busy here in the U.S. The hacks that began against HBGary spread to a separate Anonymous arm named LulzSec. For fifty days, LulzSec attacked many public and private institutions including Fox News, Senate.gov, CIA.gov, FBI’s InfraGard, PBS, AT&T, and Amazon (Wikipedia, 2011). Email accounts and passwords were released; credit card information compromised; and websites defaced. Each day, it appeared the InfoSec industry, hacker community, and tech journalists anticipated what LulzSec would release and
how companies and government would respond. Meanwhile, the Twitterverse was flooded with
new hash tags as well as raw, satiric updates from the new Anonymous arm.

As more journalists began paying attention to LulzSec, headlines ranged from, “Is there a
hacker epidemic?” to “LulzSec threatens government” naturally evoking, or at least attempting
to evoke, a sense of public fear. But were the headlines justified? And if they were justified, for
whom?

World-renowned security expert Bruce Schneier responded to whether there was a
hacking epidemic writing,

“The apparent recent hacking epidemic is more a function of news reporting
than an actual epidemic. Just because the average person reads more articles
about more events doesn’t mean that there are more events - just more
articles…None of this is new, none of this is unprecedented. To a lot of
security professionals, the value of some of these groups is to graphically
illustrate what we’ve been saying for years” (Schneier, 2011).
While LulzSec churned out many hacks, this was nothing new. One of the very first, infamous hacks was the WANK worm deployed in 1989 that propagated on the DECnet, a network shared by NASA and the U.S. Department of Energy, that froze all infected computers and took weeks to remove (Dreyfus & Assange, 1997). What was new, however, were the concentration of hacks within a brief time window plus LulzSec’s incredible knack for publicity that created an easy story for media hype. Yet, this does not mean their actions and the implications are unworthy of scholarly analysis and InfoSec corporate policy evaluation.

**Corporate and Political Governance: Reviewing InfoSec policies**

In the mid 1980’s the American automobile industry was transformed when activists working within the industry mobilized. Unlike other countries, the auto industry in the U.S. overlooked quality and innovation concerning quality circles. For workers, this meant the possibility of working for a weakened industry in a global economy and, in the long run, facing unemployment. It was only after mobilization by the workers that subsequent reforms, such as quality institutes and initiatives as well as the establishment of the Baldrige Award, were actualized (Rao, 2009). The lessons learned from the auto industry can also be applied to the evaluation and revaluation of information security policies in corporate arenas when the strikingly similar parallels are examined.

After HBGary suffered hacks by Anonymous, the company’s business partnerships suffered. The most striking example is Palantir and Berico Technologies decision to sever their relationships with the compromised corporation. Just as Palantir had generated hundreds of millions of dollars selling high-end data tools to governments and other agencies (Wired, 2011), Berico Technologies secured U.S. army contracts also worth hundreds of millions of dollars
These contracts and partnerships are no longer accessible to HBGary, translating into lost opportunity on future gains they will never see.

Not only has their business suffered financially, they are also under investigation by the House Armed Services Subcommittee on Emerging Threats and Capabilities. The congressional probe seeks data on contracts HBGary and its partners hold with the U.S. military and NSA. (Wired, 2011). The consequences of federal investigation are extremely dire. Other government and private agencies may opt not to partner with the security firm given their poor reputation and this, in turn, translates into less opportunity in the global market place. So how can other corporations escape a similar security breach to avoid embarrassment? Speaking strictly from a corporate view on policy and governance and not the compromised ethics exhibited by HBGary, it is by reviewing their corporate policies on information security.

Whitman and Mattord (2010) describe InfoSec performance management measures that determine the effectiveness of the execution of information security policy; the effectiveness and efficiency of the delivery of information security services; and those that assess the impact of an incident or other security event on the organization or its mission. Similarly, they ask what basic, risk strategies are organizations choosing to control such risks. Is it avoidance, transference, mitigation, or acceptance? These strategies are, of course, dependent on the organization and the industry it operates within; however, these decisions and considerations are an exercise all organizations must endure.

**Smart Mobs, Market Rebels, and Culture Jammers**

While organizational information security policies provide corporations and government agencies with preventive and responsive procedures, there are external factors that information security policies are unsuited to handle. Many information security departments, specifically the
title-less individuals working in them, may not understand the extent to which the larger organization they work for are involved in corrupt practices. Therefore, no matter what InfoSec policies are in place, if an organization is colluding with others in the creation of an unjust and undemocratic political, financial, and legal system, it is subject to ultra-coordinated motherfuckery in the virtual space. But perhaps virtual disobedience alone is not concerning.

Evgeny Morozov (2011) criticizes proponents of social media who extol virtual platforms as the only explanation for the success of revolutions; and he is right. Virtual networks alone do not ensure the success of revolutions; however, they do facilitate mobilizations that help their success. The critical change is the way information can quickly travel between people. The once wide “time cushion” described by Lerner and Koehler (2007) has narrowed, allowing rapid updates on critical events. Similarly, the diffusion of innovations model by theorist Everett Rogers, explains how the spread of information through homophilous and heterophilous links expedites the formation of a critical mass. Collective actions are also developed and nurtured through what Rao (2009) calls “hot causes” and “cool mobilizations” where the former describes the fostering of deep, reciprocal emotions while the latter emphasizes how “communities of feelings” are generated. Creating these feelings are the culture jammers, an instrumental technoculture who produce video, audio, and other media artifacts (Dery, 2003).

With all elements working in tandem and under the right conditions, we are witnessing a new breed of civil disobedience – one set in motion by its “Generation Text” predecessors (Rheingold, 2002) and sustained by its progeny. It is the amalgamation of civil disobedience in virtual and physical spaces. The Arab Spring has made an indelible mark on history, Spain’s Indignados marches have had a half million participants, and Occupy Wall Street is entering its second month. What started as a call from Adbusters, the occupation demonstrations have grown
to hundreds of cities worldwide and are being assisted by Anonymous. Like the movements before Occupy Wall Street, Anonymous is contributing dedicated server spaces, offering encryption advice, and protecting journalists who live-tweet marches from inflammatory comments by other Twitterverse users. They are also doxing (providing personal information) on officers who brutally attack nonviolent protestors and although there have not been successful reports of DDoS attacks on specific websites, the possibility should not be ruled out.

**Predictions anyone?**

Predicting outcomes from the Arab Spring and Occupy Wall Street demonstrations are impossible to declare with certainty. Yet, corporations and government must grapple with this uncertainty if they are to survive as legitimate, 21st century institutions. Legitimacy in the digital, information age will not be defined by what *is* but what *will be*. What *will be* the shareholder’s response when millions in executive pay are doled out to their CEO while their workforce revolts because their wages are frozen? What *will be* the politician’s decision when revolts responding to the erosion of civil liberties and the corrupt banking cartel arise? As we see unfolding all around us, a traditional response is no longer tolerable evidenced by what began in the Philippines in 2001 and what continues in demonstrations and occupations around the world. While some corporations and governments seem to be taking ethically centered initiatives, the message for those who do not is simple. We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect Us.
References


