Discipline & Index:
The Tension Between Control and Freedom on the Internet

by Chelsea Palmer, 2015

The Roots of Power, Control and Resistance in the Information Age

Community Psychology analyzes macrosystems, as found in the interaction of larger institutions and forces in society (Bronfenbrenner, 1994). Similarly, Michel Foucault's work was a study of such social systems at various points in history, with a particular focus on their effect on individuals' behavioural practices (Gillan & Lemert, 1982). Approaching history with the larger picture in mind creates an ideal opportunity to track the larger tension between top-down institutions and the grassroots communities which may either support or resist those institutional forces. Community Psychology also accounts for the "'dynamic equilibrium'" of these systems, which is particularly vital to understanding the influence of contested ground between state-led powers and activist communities (Rappaport, 1977, p. 155).

There has been a push and pull between government funding and academic pioneering since the very origin of computer technology. During the World Wars of the early twentieth century, dominant nations engaged in conflict raced to advance their mechanical capabilities for encryption, decryption, and surveillance (Winston, 1998). Following these wars, the rapid development of ever-faster and ever-smaller computer hardware components continued for decades. As the Cold War intensified, the US Department of Defense shifted its attention to the possibility of implementing a decentralized communication system in case of nuclear combat. As a result, the venture of a data transmission network called "ARPANET" was funded, with the development largely delegated to secondary academic institutions where research into local area networks had already started (Curran, 2009; Brunton, 2013).

Some of the researchers who helped create ARPANET went on to work at major technology corporations, bringing their experience and thus triggering the first steps toward private development of network capabilities (Hughes, 2004). As these efforts became more visible, enthusiasm spread amongst computer hobbyists and early adopters, so that by the 1980s, the progress of these transfer networks was largely in the hands of the earliest "hackers," or dedicated programming enthusiasts (Thomas, 2005; Brunton, 2013). The grassroots utilization of dial-up modems over telephone connections, and the establishment of collaborative bulletin board systems, cemented the independent establishment of an open network infrastructure that spread like wildfire (McKinnon, 2012).

In 1995, at the CERN research facility, Tim-Berners Lee produced the prototype for what would become the World Wide Web that we use today (Chodos, Murphy & Hamovitch, 1997). The possibilities of the Internet were continuing to expand beyond the purview of centralized government design. The rich tradition of user-led development, in which products are tweaked by individuals to suit their needs and overcome limitations, has consistently led movements in the larger industry and shaped the progress of the information technology field (von Hippel, 2011). The evolution of the Internet illustrated a push-and-pull between the governmental aims of its inception, and the vision of a free and open realm of "many-to-many communication" (Chodos, Murphy, & Hamovitch, 1997, p. 55).

Control: Internet Surveillance and Increasing Restrictions Upon Online Freedoms

Contrary to popular opinion, the recent upsurge in centralized surveillance is not the result of corporations or governments gaining more interest in tracking citizens. They have always been motivated to monitor populations as thoroughly as possible, but only recently have we developed the technical capabilities for the level of sophistication we see in GPS tracking, ubiquitous closed caption recording, and the establishment of ever-expanding databases (Soltani, 2013). The transition from explicit observation to "dataveillance," in which complex profiles of each individual are compiled based on the data traces of their activity, has changed the game, as far as privacy and autonomy are concerned (Bady, 2011). A crucial component of surveillance and tracking lies with devices' output of metadata, information attached to media which gives specific information about the origin of those files (Vaidhyanathan, 2011). The tracking of individuals' movements, the content of their telecommunications and correspondence, and databases of their physical appearances are all being utilized by governments under the guise of fighting crime and terrorism (Lauer, 2011).

The development of surveillance and location tracking technology is briskly evolving. For example, RFID chips, which are tiny microchips utilizing radio transmission signals to broadcast an object's location, are being gradually incorporated into passports and other forms of citizen identification (Hayles, 2009). Last year, the FBI launched a highly accurate facial recognition system in the United States, and they are compiling a massive database which will include cross-reference to identifying bodily marks and descriptors (Pagliery, 2014). Canada is not far behind, as the federal government continues to push for looser restrictions regarding the collection and use of biometric data (Mas, 2015). Major companies like Google and Microsoft have vocalized their opposition to NSA surveillance programs and other apparent transgressions against citizens' data privacy (Zetter, 2014). Interestingly enough, these technology corporations are less transparent about their own practices of dataveillance and customer profiling.

Most users might think they need to have the satellite setting turned on for their phone's location to be tracked. In reality, companies like Google have been perfecting "peer-to-peer" location finding for nearly two decades, in which device locations are extrapolated and logged by triangulating their data connection and their proximity to area WiFi networks (Madduri, 1998). Rather than questioning these private corporations' surveillance strategies, the United States government has demonstrated its intention to follow their example and adapt these technologies, both to track users and to perform analyses of the larger population's online activities (Baron, 2009; Vaidhyanathan, 2011).

Werbin (2011) investigates the effects of the intelligence community's increasing use of data mining, and the way that these practices influence and shape the behavior of the profiled targets. As we grow more accustomed to sharing data about ourselves and our movements through social media interfaces, we begin to shape our behaviour to fit into the norms of those platforms. Once we decide to leave our satellite GPS tracking turned on and publically visible, it follows that we would "log" our travels, "checking in" at various locations and broadcasting our public movements and actions. Once we've internalized the concept that our memories belong on Instagram, posted a mere moment after we make them-- once we're used to parsing Facebook events to figure out what's going on in our communities and social groups-- once we automatically Google every question that pops into our heads, no matter how fleeting-- it becomes an effortless task for monitoring to compile all of this information into centralized databases.

Some of the most vocal critics of the US government's subtle but totalizing surveillance efforts are smaller companies that are at the forefront of developing independent security technologies. In particular, industry watchdogs have attempted to expose the FBI's potentially unconstitutional use of International Mobile Security Identity catchers [IMSI-catchers], which allow agents to eavesdrop on mobile devices remotely, while presenting the appearance of a functional cell phone tower (Soltani & Timberg, 2014). In California, an investigation showed that both the San Bernardino and the Sacramento Sheriff's Departments had used IMSI-catcher technology extensively without obtaining appropriate warrants, a circumstance about which they still refuse to release documented confirmation or denial (Farivar, 2015a; Farivar, 2015b). With the constant obfuscation of these behind-the-scenes practices, it is no wonder that many Internet activists have taken it into their own hands to uncover information and disrupt surveillance practices.

White Hat/Black Hat: Hacktivism, Whistleblowers, and Subversive Resistance

Since the origins of the Internet, some of its most skilled users have employed their computers not just as relays for communication, but as unique tools for disruptive action. "Hacktivism" is, in its simplest definition, civil disobedience utilizing technological platforms (Karatzogianni, 2004). In general, hacktivists aim to counterbalance or fully undermine what they see as the oppressive impact of totalizing control enacted by governments and global corporations (Söderberg, 2013). Hacktivists pursue the radical disruption of centralized data systems and websites, and take advantage of tools to ensure their actions remain untraceable and anonymous (Kushner, 2013). Though there is often a great deal of solidarity for hacktivist movements online, by their very definition they are loose affiliations, with both blame and acclaim belonging to everyone and no one at once. Hacktivists can employ light-handed tactics that merely aim to gain the media's attention, or they can engage on a much more destructive front by penetrating security systems and wreaking havoc.

WikiLeaks began in 2006, set in motion by an ideologically motivated hacker named Julian Assange (Pontin, 2011; Birchall 2014). The project's intent was to track down information and documents about government and military operations which Assange saw as abuses of power or elements of authoritarian conspiracy (Assange, 2006). By 2010, WikiLeaks had gained widespread recognition. One of its better known releases was a video demonstrating a callous overuse of force in a Baghdad airstrike, which resulted in death and injury to innocent bystanders (Assange, 2010). Obviously, such leaks garnered extreme but mixed reactions from the general public (Lindgren & Lundström, 2011).

Pontin (2011) expressed a mixture of skepticism and grudging respect for the driving mission of WikiLeaks, leaning more toward criticism of its potential to destabilize government operations, but endorsing the underlying vision of journalism as a force for transparency. For his part, Assange (2010) maintained that WikiLeaks was a legitimate media organization which produced crucial information in the modern, over-extended military state. He countered the popular criticism that WikiLeaks has tarnished foreign sentiments about the United States, as he pointed out that the global citizens most affected by the US military already see these abuses on a daily basis, and that it is the residents of the United States itself who have been oblivious to these war crimes perpetrated abroad.

Recently, multiple academic and government agencies collaborated to produce a study on the current state of cybercrime in the United States, finding that most organizations are woefully underprepared to deal with the skill and capacity of "black hat hackers.". Black hat hackers utilize their extensive computer skills to penetrate and disrupt security systems, generally for the purposes of crime, pranks, or to make extreme political statements (Thomas, 2005).

Numerous US police departments have fallen prey to "ransomware" attacks, in which black hat hackers encrypted all of their systems' data and refused to release it until they were paid a fee in untraceable Bitcoin (Bray, 2015). Similarly, the US State Department was unable to exorcise a group of Russian hackers from their email system for three months, as every time they resolved a security breach, another immediately popped up (Thomson, 2015). Internationally, a group of hackers of unknown origin managed to siphon millions of dollars from banks all over the world in what was clearly a complex and long-running attack, involving multiple layers of malware dissemination, identity impersonation, and alteration of digital records (Sanger & Perlroth, 2015).

On the other end of the spectrum, "white hat" hackers aim to expose security flaws in systems in order to help fix and strengthen them (Thomas, 2005). One white hat hacker recently uncovered a breach in Facebook that would have allowed him to delete every photo that had ever been uploaded to the site (Stockley, 2015). Luckily for Facebook's user base, rather than following through with this threat for laughs, he contacted Facebook and was able to secure a monetary reward through their "bug bounty" program (Muthiyah, 2015).

Bug bounties are offered by most major online companies, as an incentive for hackers to come forward with system flaws instead of exploiting them. There is significant debate regarding whether this has actually made the Internet more secure, but it is generally agreed upon that it creates a more amiable climate between corporations and hobbyist hackers (Zetter, 2012). At the end of the day, cybersecurity experts are most likely to build successful protective measures by thinking like a hacker, and turning black hat tactics against their perpetrators (Bloomberg, 2014).

On the much more informal and immature side of the Internet is the long-standing community of 4chan. 4chan is best known on the Internet for its combination of anonymous forums and its users' significant pooled resources of technological capital (Dibbell, 2010). In other words, 4chan has a higher-than-average population of skilled hackers. Collaborative actions originating on the site can range from white hat protest campaigns to black hat harassment and pranks. The site is raw and unfiltered, and its user base can be aggressive and combative to apparent newcomers, who they identify primarily by an inability to follow 4chan's intensive insider jargon (Poole, 2010). 4chan is just as well-known for being the origin point of classic Internet jokes as it is for being the home base of the radical hacktivist collective, Anonymous (Woolf, 2015).

When members of Anonymous intend to wage a new campaign, they launch a written message or voice-modified video, usually consisting of an ultimatum that must be met or a warning will be carried out. The organization prioritizes a non-hierarchical structure, and generally considers anyone who chooses to identify themselves or seek press attention to be self-congratulatory and egotistical (Kushner, 2014). Rather than recognition, Anonymous members claim to desire to see justice in the world, however they define it (Kushner, 2014). The collective does not rely upon leaders but instead is what Norton (2012) refers to as a "do-ocracy," in which any associated member feels complete freedom to take immediate action in the name of the larger group.

This amorphous structure inevitably leads to some silly operations, but it has also produced a few game-changing revelations. One of these was the collective's raising of the Steubenville Rape Case into national awareness: a young girl was raped by multiple football players in a small town in rural Ohio, and despite her attempts to seek justice, it was ignored by both the school and the police (Kushner, 2013). An Anonymous member stumbled across the obscure page of a Steubenville blogger who was trying to draw attention to this injustice, and soon enough, the entire country was watching, and justice was served. Unfortunately, heroic actions like these do not change the official perspective that groups like Anonymous border on terrorism.

Scapegoats and Criminals: Campaigns Against Anonymity

4chan's founder Poole (2010) pointed out that in the current age of social media, we are moving further and further towards ubiquitous persistent identity, or the fixed association of our online accounts with our legal identities. In a world where we are under the constant threat of surveillance, taking actions against perceived injustice can carry incredible risk. Anonymity is potentially the strongest tool an activist can have in the current age. As Poole himself explained, the social strength in complete anonymity is its erosion of judgment and hierarchy: "it's incredible what people can make when they're able to fail publicly without fear" (2014a). In terms of more radical politicized action, anonymity instead determines the difference between freedom and incarceration.

For many decades, the United States government has instigated various periods of "moral panic" around the existence and activities of hackers, based upon the actions of the much smaller demographic of black hat hackers who use their skills to perpetrate crimes (Thomas, 2005). This has tarnished the word "hacker" itself, through continual association with misdeeds. However, members of the community often still cling proudly to the title, because they understand its functional meaning as an indicator of technical prowess. The castigation of hackers is just one in a long series of governmental "otherings," in which a specific group is depicted as complete enemies of the state, and even misidentified as the primary threat to the safety of a nation's population. By convincing the public that they are always on the verge of victimization by these clearly delineated "enemies," the state can justify extreme and total eradication of any related campaigns of dissent.

When the possibility of anonymity is eroded, it becomes easy for institutions of power to cast a single transgressor as a scapegoat, to serve as an example of what can potentially happen to those who break established codes of behaviour. One such scapegoat was the Internet activist Aaron Swartz, who was arrested for downloading a large amount of articles from an academic database, and was then faced with decades of potential prison time (Collier, 2015). Swartz had a long history of mental illness, and the intense stress of the trial led him to kill himself (boyd, 2013). Similarly, Deric Lostutter, the driving force behind Anonymous' massive exposure of the Steubenville rape case, is now facing a potential jail sentence eight times the length of the one the convicted rapists received (Kushner, 2013). His supposed crime is hacking into social media accounts associated with the scandal, a charge he still denies. Like Swartz, he was a high-profile target for prosecuting agents who want to "send a message" to hacktivists. It seems to most members of the information technology community that the real offenses these young men committed were their challenges towards an archaic and broken system, in which information is locked away behind expensive doors and rape reports are never filed.

Willcocks (2006) points out Deleuze's effective adaptation of Foucault's disciplinary society to the concept of a control society, which relies more on material technology than physical confinement to corral and influence its population. Poster (1989) agrees that this is the most useful contemporary adaptation of Foucault, as he conceptualizes a "superpanopticon [... in which] contemporary surveillance is a product of new methods of *information* processing, not brute force" (p. 123). Poster depicts this as an inevitable extension of modern capitalism's mechanization of labour and production, as well as the increasing computerization of leisure and daily life. The omnipresence of cameras, metadata, and tracking devices exacerbates the power of centralized databases, and reinforces that "every conceivable aspect of ordinary activity leaves a trace in the memory banks of machines, and these traces are available instantaneously should the occasion arise" (Poster, 1989, p. 122). The more thoroughly we examine the possibilities available for centralized surveillance and control, the more obvious it becomes that checks and balances will be vital in this age of technology.

Finding a Balance Between Regulation and Liberation

The Community Psychology concept of "psychopolitical validity" requires practitioners to evaluate and acknowledge the complex outcomes their actions might produce within social systems (Nelson & Prilleltensky, 2010). For subversive political activism, psychopolitical validity is equally important, as hacktivists who aim to incite true social change must be wary of the ripple effects of their actions. Striking out against the structures of surveillance may sometimes result in even more stringent restrictions and laws put upon the general public. In order to truly maintain a free and open Internet, activists must carefully evaluate whether or not their actions are likely to have a net benefit, or negative consequences, for society as a whole. The organization tactics of the Arab Spring protests may be an ideal model for walking this balance effectively: tools like Twitter were employed for rapid and straightforward communication of meetings and demonstrations, and pictures and videos were uploaded to demonstrate abuses of power as they happened, but protesters did not make the mistake of identifying themselves or their specific plans via social media (AlSayyad & Guvenc, 2013). This allowed participants in the protests to utilize the best elements of the Internet without unnecessarily exposing themselves to potential surveillance.

One of the central incongruities between the current American legislative battles over Internet freedom and its actual functionality is the fact that the existing Supreme Court justices have been conditioned, in legal training, to rule by analogous equivalency, and thus they are establishing precedents around new technology which are rooted in archaic notions of censorship, communication, and creation (MacLaren, 2015). Many of those who are responsible for shaping law in the digital age don't even use these technologies in their own lives. This recalls Lahlou's (2008) point that too often, the material layer of technological devices advances rapidly, while our institutional governance of those innovations lags behind.

Guattari (2000) warned that if citizens place “blind faith in the technocrats of the State apparatuses,” computer technology is likely to be wielded to control populations, rather than to liberate them (p. 28). Of course, in order to stay one step ahead of the stifling effects of centralized control, we need the technological innovators of the current age to devote their time to solving meaningful problems. With the overvaluation of largely superficial mobile app startups, there may be too much incentive in Silicon Valley to produce flashy, rather than useful, ideas (Malone, 2015). If we encourage the innovators of the next generation to continually disrupt, rather than sustain, the current norms of technology, we can avoid the pitfalls of merely prescriptive practices that keep us stuck in a rut which is continually co-opted by institutions and corporations (Franklin, 1990; Latzer, 2009).

Gilbert & Powell (2010) explained that Foucault’s concept of possible resistance is embodied in all of the small choices an individual makes in his or her daily life. These seemingly innocuous, constantly present decisions are influenced by our notions of knowledge, our feelings of agency or powerlessness, and our response to the dominant narrative of truth in our society. Foucault himself, in an unusually cheerful interview, proclaimed that “aside from torture and execution, which preclude any resistance, no matter how terrifying a given system may be, there always remain the possibilities of resistance, disobedience, and oppositional groupings” (1980, p. 45). The issue, as it always has been in society, is finding a balance between standing up against oppression and becoming an unintentional martyr.