LEARNING FROM MAFIABOY

Gary Genosko*

On 12 September 2001, at the Chambre de la jeunesse of the Cour du Québec in the District of Montréal, Gilles L. Ouellet J. sentenced a 17-year old male hacker known by the handle "Mafiaboy" from Ile-Bizard, a suburban community near Montréal, to eight months open custody, one year of probation, and a modest fine of $250 to be donated to the non-profit organization Sun Youth. For the crimes of unauthorized use of computers and mischief in relation to data, this sentence falls well below the two years he could have served under the much less "open" conditions in youth detention. Since the time of his sentencing, not much has been written about Mafiaboy and the case has faded from view, both popular and critical alike. Without question, being sentenced the day after 9/11 guaranteed that Mafiaboy's story would be erased from the mediascape.

There are still lessons to be learned about democracy and the Internet from the Canadian case of Mafiaboy.[1] There are two specific lessons I want to underline in this short paper. The first lesson is that Mafiaboy's activities can be decoded by borrowing ideas from cultural studies and applying them to the youth subculture of computer hacking. Instead of capturing Mafiaboy's actions in a punitive discourse of cybercriminality, I give serious consideration to computer hacking as a youth subcultural practice of technological experimentation. In this respect, such practice expresses a desire to bridge by technological means the gap between social situation and positive imagined outcome. The second lesson is the dissatisfaction resulting from the difficulty in bringing forward evidence of these types of crimes. Although Mafiaboy's guilty plea ultimately rendered this evidence unnecessary, a lack of transparency on the part of the wronged parties with regard to the precise nature of their actual damages clouded the case's value, much to the Judge's displeasure. Both lessons are gleaned from the Judge's sympathetic opinion of Mafiaboy and the lightness of his sentence.

For those who have already forgotten what the fuss was about, a brief review of this case, the only one of its kind in Canada, is in order. During the week of 7 February 2000, the websites of blue chip e-businesses, including Amazon, CNN, Dell, eBay, and Yahoo, buckled under the weight of a furious wave of Distributed Denial of Service (DDoS) attacks executed by Mafiaboy through hijacked computer networks of American universities. A DDoS attack "floods" sites with data packets[2] with which they cannot cope: Mafiaboy had planted a number of Denial of Service agents on hijacked computer systems at American universities in California and

---

* Dr. Gary Genosko is the Canada Research Chair in Technoculture in the Department of Sociology at Lakehead University, Thunder Bay, Ontario.

[1] *R.* c. *M.C.*, [2001] J.Q. No. 4318 (C.Q. jeun.) (QL).

[2] Essentially a bombardment of the computers housing the websites with data requests.

Massachusetts – and remote-controlled the operation with a "rootkit",[3] using the captured computers to execute the attacks.

The situation for e-commerce at the time was already volatile. Jitters about Y2K had not fully subsided, and viruses attached to email messages haunted the Webscape, but the deflation of the dot-com bubble after its peak in March 2000[4] unquestioningly intensified the pursuit of Mafiaboy; the case of *United States v. Microsoft Corp.*[5] was beginning to issue market unfriendly findings, and media takeovers of gargantuan proportions were occurring.

The U.S. Attorney General's office under Janet Reno brought these DDoS attacks to the attention of President Bill Clinton; subsequently, the Director of the Federal Bureau of Investigation (FBI), Louis J. Freeh, began claiming that Canada was a "hacker haven". The attacks also tested the mettle of the heavily upgraded and retrained cyber-cops of the U.S. National Infrastructure Protection Center (NIPC) and the Royal Canadian Mounted Police (RCMP). There is no general agreement about the "digital correctness" of DDoS attacks – they are often dismissed as low-level vandalism, but may also serve as collective acts of protest; that is, genuine examples of "hacktivism".[6] During and immediately following Mafiaboy's pursuit by FBI and Canadian Security Intelligence Service (CSIS) agents, and his arrest in April 2000, his so-called peers in the digital subculture were not very delicately excoriating him as a "packet monkey" and "script kiddie", two disparaging terms for amateurs who do not write their own script (set of computer commands) but instead buy it from somebody else and then use it in a malicious way. The two Kevins, Mitnick (aka Condor) and Poulsen (aka Dark Dante), well-known former hackers now serving as technical experts on e-security, criticized Mafiaboy on technical grounds.[7] To them, he was no better than a spammer. The counterpoint to these criticisms, as well as those leveled by security experts and law officials, was anti-globalization journalist Naomi Klein's posting of "My Mafiaboy", a letter to the young hacker.[8] Klein's tongue-in-cheek posting took exception to the quick verdicts of Mitnick and others: for her, Mafiaboy was a kind of anti-corporate freedom fighter within the anti-globalization movement; he was "committing an act of love...not for the integrity of a particular line of code, but for the Internet in general".[9]

---

3 Term given to collection of software tools installed by an intruder on a compromised computer to hide evidence of the intrusion and create backdoors to allow future access or remote control of the computer.

4 In terms of the rise of the NASDAQ Composite Index.

5 *United States v. Microsoft Corp.*, 87 F.Supp. 2d 30 (D.D.C. 2000).

6 The term "hacktivism" is commonly given to mass political activism through electronic means.

7 See Kevin Mitnick, "The World's Most Hunted Hacker" *Time* 155:7 (21 February 2000) 21; Kevin Poulsen, "Free Mafiaboy" (24 April 2000), online: SecurityFocus <http://www.securityfocus.com/>.

8 Naomi Klein, "My Mafiaboy" *The Nation* (13 March 2000), online: The Nation <http://www.thenation.com/doc/20000313/klein>.

9 *Ibid.*

While Mafiaboy was subject to the to-and-fro rocking of the media phantasmagoria, his lawyer, Yan Romanowski, was developing a strategy for his defence. RCMP computer crimes investigators and Crown prosecutors had already indicated to the press that the wiretap evidence they possessed of Mafiaboy's intent to commit computer fraud and data mischief was overwhelming and beyond any reasonable doubt. Still, the legal defence strategy that emerged during the pre-sentencing hearing met the question of intent head on with the counterclaim that the accused was testing the security of the websites in question. The defence argued that the accused's motive was "public service", not malicious damage. As the trial began in late June, Mafiaboy entered a plea of guilty with the proviso that he was a "white hat" hacker[10] conducting "experiments" that would ultimately help selected websites improve their security systems. His hacks provided proof of security problems and were also helpful in providing solutions to such problems; it was a simple trick: expose the fault and then deliver the solution. The point of Mafiaboy's experimentation was to land him a position as a computer security analyst. Evidence from his appointed social worker, Hanny Chung, suggested that while Mafiaboy identified with the "white hats" and wanted to share the results of his experiments in order to secure a position as a computer security analyst, his subsequent and repeated actions undermined those stated beliefs. A concerted DDoS attack is not the sort thing a "white hat" would launch.

Lesson One

Ouellet J. responded like a seasoned decoder of youth subcultures. He explained, in fact, that his strategy was not to dwell on intent, but rather to focus on motivation. The judge concluded the defence argument that Mafiaboy was only "conducting a test" with the aim of winning a position or developing better firewalls had more the air "*d'un prétexte ou d'une excuse que d'une réelle motivation* (of a pretext or an excuse rather than a real motivation)."[11] Using the language of Birmingham school cultural studies,[12] Ouellet J. took up the power of the imaginary solution against its unlivable reality:

> *Bien sûr, en arrière plan, il n'est pas exclu que l'adolescent ait pu entretenir ce rêve ou pensée magique qu'en réalisant ce qu'il considérait comme un exploit, comme un 'grand coup', il verrait ses talents reconnus et que tous se précipiteraient pour lui offrir de l'emploi. Mais dans la réalité de tous les jours, la véritable motivation de l'accusé était de tester ces sites, non dans le sens de conduire une expérience, mais dans le sense de défier et vaincre ces systèmes, pouvant s'enorgueiller d'une éventuelle réussite et en retirer crédit aux yeux de la communauté des 'hackers' principalement.* (Certainly, in retrospect, it cannot be ruled out that the youth cultivated this dream or magical thinking that, in carrying out what he considered to be an exploit, 'un grand coup', his talents would be

[10] In contrast with a "black hat" cyber-criminal who hacks with malicious intent.

[11] *Supra* note 1 at para. 4 [translated by author].

[12] John Clarke *et al.*, "Subcultures, Cultures, and Class" in Ken Gelder & Sarah Thornton, eds., *The Subcultures Reader* (New York: Routledge, 1997) 100.

> recognized and this would lead to job offers. But in everyday reality, the real motivation of the accused was to test these sites, not in the sense of performing an experiment, but in the sense of attacking and conquering these systems; boasting about his eventual triumphs would enhance his reputation in the eyes of the hacker community.)[13]

The Judge's explanation for Mafiaboy's true motivation was peer recognition, going so far as to offer his opinion that an "experiment" would not have required such an elaborate use of zombie networks.

Mafiaboy may have also discovered that his imagined future as a hacker legend or corporate security employee was incommensurable with his everyday reality as a computer-loving teen whose curiosity passed over into mischief and beyond. The choice of unreality over reality is common to group fantasies among youth subcultures. It is a magical resolution of the inherent contradiction in breaking security systems in order to be welcomed into the computer security fold; it allows one to live a dream of peer recognition and celebration, of employability, and even of personal freedom, while sitting alone, before the screen, still a teenager living with one's parents in the suburbs. Early work on youth subcultures undertaken within the Birmingham school of cultural studies emphasized the role of subcultural style and ritual behaviours as means of working out "magical" or "imagined" resolutions to socio-economic predicaments and inter-generational contradictions that would have otherwise remained hidden.[14] The "imaginary solution" is quite "unlivable"[15] even if for a time, the prospect of wearing the "white hat" of a Master hacker by bringing down popular websites pushes reality aside. This was not lost on the Judge, though Mafiaboy's wishfulness, and the precedence he gave to unreality over reality, ultimately did not stand up to the youth justice system, to the necessity of high school, and to subsequent entry into the meritocracy. Still, this does not mean that late at night, in his bedroom, before the screen, Mafiaboy had not won for himself a space away from the dominant culture.[16] But in this space, he would not find an enduring solution to his predicament, especially through the symbolic mantle of untouchable Master hacker. His attempts at a more concrete solution through the demonstration of his skill certainly played in the media for a brief but intense season, but they did not play out as a viable answer to the problem of career choice and entry into a profession.

---

[13] *Supra* note 1 at para. 4 [translated by author].

[14] *Supra* note 12.

[15] Dick Hebdige, "The Function of Subculture" in Simon During, ed., *The Cultural Studies Reader* (New York: Routledge, 1993) 442; Dick Hebdige, "The Meaning of Mod" in Stuart Hall & Tony Jefferson, eds., *Resistance Through Rituals* (London: Hutchinson, 1976) 87.

[16] Although hackers consider bragging on Internet Relay Chat to be totally "lame"; see Douglas Thomas, *Hacker Culture* (Minneapolis: University of Minnesota Press, 2002) at 139.

Lesson Two

The spectacular and hyperbolic assessments of the economic damage caused by Mafiaboy's DDoS attacks lead to the second lesson. In a case such as this, it is difficult, if not impossible, to pinpoint the precise extent of the damages caused by the accused's actions. Estimates of revenue losses, losses in market capitalization, costs for upgrading security holes, and costs of repairing consumer confidence are arrived at by speculation and extrapolation. These "costs" are quite intangible, so much so that companies cannot accurately quantify them. They represent potential losses rather than the actual damages sustained. The escalation of cost claims across the media reports, from millions through hundreds of millions to billions, was neither justified nor explained by the companies or the media. However misleading, metaphors seemed to suffice: the engine of the North American economy was being stalled by hacking; hacking can be blamed for the bursting of the e-bubble economy. Certain large numbers were produced by third parties like the Boston Yankee Group, which cited a figure of $1.2 billion U.S., but they lacked foundation.[17] Such big numbers were consonant with both the shock of this first big *wave* of DDoS attacks on established names, and the attention they attracted as events unfolded in the highly charged atmosphere of highs and lows on the NASDAQ Index. Those numbers did not enhance Mafiaboy's reputation among his peers, but instead attracted a united North American intelligence response. One wonders how much notice a low-grade technical attack, easily traceable through router logs, would have received without these inflated damage reports. They didn't impress the Judge as even he notes that not one of the vendors suffering a loss came forward to quantify that loss; this lack of cooperation concerned him, especially in light of the delirious media speculation about the case.[18] The Judge's opinion was that computer crime cannot be successfully fought in the absence of cooperation and collaboration between victims and police: *"il est déplorable que ces sociétés n'aient pas fourni une meilleure collaboration aux autorités policières* (it is deplorable that these businesses did not make a greater effort to collaborate with police agencies)."[19] This opinion has motivated the RCMP to build better contacts with Internet Service Providers (ISPs) whose normal practice is to quietly close accounts rather than report incidents of hacking. The Mafiaboy case is cited by the RCMP as a primary example of the need for an effective strategy given that "before [the big wave of DDoS attacks] four Internet accounts registered to Mafiaboy's residence were terminated for hacking activity by three separate ISPs. Hacking activity from these accounts was never reported beyond the individual ISPs."[20]

---

[17] Research consultancy groups like Yankee serve the interests of their clients, even when they issue press statements; Yankee is owned by a private equity firm specializing in telecommunications. See online: The Yankee Group <http://www.yankeegroup.com>.

[18] *Supra* note 1 at para. 7.

[19] *Ibid.* [translated by author].

[20] Royal Canadian Mounted Police Criminal Intelligence Directorate, Criminal Analysis Branch, "Hackers: A Canadian Police Perspective, Part 1" (2001).

In my estimation, Ouellett J. did not go far enough in providing guidance on how to build cross-institutional and transparent cooperation to combat cybercrime; despite his criticism of the e-commerce companies' silence,[21] he admits the legitimacy of false excess (inflated damage estimates) in the media maelstrom. Real gains in this fight will continue to be precluded as long as short-term gains are achieved through both willful misdirection in the form of groundless and inflated damage estimates, and the failure of computer hacking victims to deflate the promotional spiral of these wild estimates by pursuing damage claims in court. The short-term damage is that justice is served by other means, the absence of critical counter-assays is institutionalized, and the passage from bad press to genuine success in the battle against cybercriminality cannot take place in the undemocratic court of popular opinion or on the uneven playing field of the North American media. In the game of confidence building in the e-transactions market, it is not in the interest of e-commerce operations to present accurate reports of damages suffered by system breakdowns, regardless of cause, because it may expose a level of risk that is unbearable, even for the core customer base. It needs to be acknowledged that this result contributes neither to the understanding of youth subcultures around computing, nor to building bridges between security and other interested agencies in a publicly accountable manner.

In summary, the first lesson opened the case of Mafiaboy to an expanded field of cultural understanding of youth practices around information technologies that forms the necessary backbone to an effective analysis of the real threats of cybercrime in the digital age. The critical and sympathetic understanding of the "imaginary" bridge that a hack erects across the divide between teenage alienation and mature adulthood, between a McJob and a career, is vital to fully appreciating the motivation of young hackers. The second lesson exposed a weak point in the system of prosecuting cases of this type, demonstrated by the fact that the Judge's call for cross-sector cooperation in the fight against cybercrime rings somewhat hollow in this case.

---

[21] *Supra* note 1 at para. 7.