FCJ-057 The Case of ‘Mafiaboy’ and the Rhetorical Limits of Hacktivism

Gary Genosko, Lakehead University, Thunder Bay, Canada.

2 > Canada proved to be the home of the most notorious Web hacker to date, “Mafiaboy,” a Montreal teen who intermittently crippled the Web sites of Amazon, CNN, Dell, eBay, and Yahoo! from 7-15 February 2000 by means of a distributed denial of service attack in which Web servers were flooded with so many requests for data that they were effectively clogged. He was charged under subsections 342.1(1) (unauthorized use of computer) and 430(1.1) (mischief in relation to data) of the Criminal Code (R.S.C. 1985, c. C-46) and sentenced on 12 September 2001 to eight months detention plus one year probation (R. c. M.C., [2001] J.Q. no. 4318 (C.Q. jeun.) (QL)).
>
> 3 Craig McTaggert (2003, at para. 81, note 112)

Introductory Remarks

4 On September 12, 2001, Cour du Québec, Chambre de la jeunesse, District de Montréal Judge Gilles L. Ouellet sentenced a 17-year old male hacker from Ile-Bizard, a suburban community on a small island (“West Island”) immediately southwest of Montréal, known by the handle Mafiaboy, to eight months “open custody,” a year’s probation (with restrictions on Internet usage and types of software), and a modest fine of $250 (due to bail violations while awaiting trial) to be donated to non-profit organization Sun Youth. Mafiaboy was 15 years of age when his crimes were committed. This sentence fell well below the potential two years (not to mention larger fine and longer probation) that would have been served under much less “open” conditions in youth detention. Since that time not much has been written about Mafiaboy and the case has faded from view, popular and critical alike.

5 During the winter and spring of 2000, this groundbreaking case of cybercrime in Canada made national headlines, preoccupied the U.S. Attorney General’s office, was brought to the attention of the President of the United States by the Director of the Federal Bureau of Investigation, and tested the mettle of the heavily upgraded and retrained cyber-cops of the Federal Bureau of investigation (FBI) and Royal Canadian Mounted Police (RCMP). The highest profile of Mafiaboy’s hacking exploits against blue chip American Web sites took place in February 2000, even before Y2K jitters had fully dissipated. Indeed, mid-February witnessed the “high-tech summit” at the White House where President Bill Clinton announced new funding and program initiatives to battle cybercrime; counted among such problems was a certain suspect named ‘Mafiaboy’ (Schwartz and Cha, 2000). Mafiaboy’s arrest in mid-April did little to calm e-commerce nerves as a mere few weeks later saw the emergence of the latest in a series of rampaging and mutating viruses – “ILOVEYOU” – spread by an attachment through Microsoft’s Outlook Express email software.

6 For those interested in cybercrime in Canada and beyond, critical attention during the nervous first spring of the new millennium lurched between Montréal and Manila as first a Canadian teenager (local Montréal press underlining that he was an “Anglophone”) and then a twenty-something Filipino, Onel de Guzman, were apprehended with great fanfare. The differences, though, were striking. Mafiaboy was legally still a “youth” under Canadian law and could not be named; this fact was respected in the US and elsewhere. In one sense, the need to constantly repeat his handle accounted for the proliferation of ‘Mafiaboys’ across the World Wide Web, which also complicated the investigation. Importantly, it took US and Canadian investigators two months to identify and finally arrest Mafiaboy (on the strength of several kinds of wiretap evidence), whereas De Guzman was discovered and arrested in a mere 7 days.

7 If you’re ever caught in the middle of a digital dispute or are accused of online misconduct, don’t make the mistake of waiting too long to get expert advice. From my own legal ordeal, I can say having a cyber crime lawyer for internet fraud defence and legal guidance was what kept things from spiralling out of control. They knew how to handle authorities, understand data trails, and explain everything in terms I could understand. Not all legal help is built for modern tech issues, but this certainly was.

8 Technically these episodes are vastly different, but their drama is structurally the same: it is built around the gap between authentication and identification, the time-span of which is limited before the computer event (the virus, the hack) is linked to an offline body; indeed, each time a major

virus such as Melissa (1999), ILOVEYOU (2000), or Anna Kournikova (2001) circulates, the drama of detection is measured in decreasing increments, and wild speculation proliferates about the number of computers infected and users affected, not to mention costs in dollars to remedy the situation and the percentage of systems shut down (value judgments about a code's maliciousness). The goal from the hacker's perspective is to maintain anonymity (uphold the handle's noncommunication with an offline identity) or defer their apprehension and, as detection time diminishes, to write program language that leaves less and less of a signature, an identification, a style recognizable by investigators steeped in tracking bugs and analyzing lines of code. This is how De Guzman was found: his strings were linked to a Filipino cell of programmers GRAMMERSoft (Greenberg, 2000). Mafiaboy's exploits did not fall into this search for a signature in script; some critics describe the aesthetic and poetic components of program language (Aarseth, 1997:11), but Mafiaboy lacked such a style; some claimed he had no style at all. He wasn't a programmer. He acquired an automated "rootkit" written by somebody else and then set it to work "anonymously." Mafiaboy executed a Distributed Denial of Service Attack (DDoS) – a "flood" of messages (packets) that by volume alone disabled servers unable to cope with the demands placed upon them – with borrowed script, in this case, a denial-of-service program authored by "Sinkhole" (although early press reports fingered a creation by a "mixter" called Tribal Flood Network). He planted a number of DOS agents on "zombies" – hijacked computer systems at universities, and remote-controlled the operation with his automated software, using the captured computers to inundate selected Web sites with data packets (numbered chunks of files). The sites included some of the biggest e-commerce operations such as eBay, Amazon, Etrade, Dell, Yahoo!, and CNN. The events of February 7-15 were, as Chandler (2003-04: at para. 15) remarks, "the Internet's first big wave of DDoS attacks."

9 The articles on the Mafiaboy case and related technical and social phenomena written by Kevin Poulsen, a former high-profile US hacker convicted of espionage but now a computer security analyst, are especially insightful. Poulsen (2000) cut to the quick: 'He was just a young teen who allegedly got a hold of some pre-fab DDoS tools and, whipped into a frenzy by the .com attacks that were already grabbing headlines worldwide, launched a copycat assault of his own. He stupidly bragged about it on Internet Relay Chat (IRC). He behaved like a 15-year-old.' A few years later, Poulsen (2003) pointed out that spammers have resorted to the 'adolescent hacking techniques' of those launching DDoS attacks. Poulsen's point was the fact that the suspect turned out to be a 15-year-old teen was embarrassing in light of the so-called closing of what has been called "the knowledge gap" between the computer security industry and computer underground (Taylor, 1999: 78-81). The gap, it seemed, closed around a technically low-level and much derided kind of knowledge that fell far short of the "Mastery" that a brilliant hack (or "exploit") would radiate (Turkle, 1984: 232). In short, the gap didn't really close very much if this was all the security forces had learned. This is an important indication of the extent to which the case of Mafiaboy is a lesson about the artificiality of persuasive language and the limits of so-called "critical" categories.

10 Early in the Mafiaboy case, suspects were characterized in terms of how they took credit for their 'hacking prowess' (Schwartz and Cha, 2000). However, Mafiaboy didn't fair too well in peer review, although he excelled in adolescent boasting. He was labelled a "script kiddie" or "packet monkey." Both terms are derisive and place him down low on the skill level admired in the hacker underground; indeed, he was caught bragging to other "script kiddies." He was "lowly" and a "kiddie" to his hacker peers because he didn't write his own code; he was not so low as to escape notice, however, yet the fact of his discovery and arrest because of his bragging about his exploits conformed to a standard motivation for hacking in the first place (peer recognition; Taylor, 1999: 59-61), even if this was also seen as carelessness; one technician at University of California Santa Barbara, the site of one of Mafiaboy's zombie networks, described Mafiaboy's work as "sloppy" and he "left an obvious trail" (Vise and Cha, 2000). Investigators simply required the ability to analyze router logs of captured computers (at the University of California and University of Massachusetts) and thus trace the link back ("from…to") to other hacked machines and a Canadian Internet Service Provider (ISP), and provide a profile of the behaviour of an account. Forensic analysis of router logs is a common practice in computer security circles. For a seasoned hacker/analyst like Poulsen, this was hardly state of the art knowledge, and did not warrant the status of a "milestone" in efforts to battle cyber-crime, as the FBI insisted. In some respects, then, the story of Mafiaboy was more virtual than reality. What makes the case compelling is that the categories and distinctions

developed in the academic literature on hacker culture fit too perfectly the Mafiaboy case and circulate with ease across defense and prosecution lines, yet upon closer inspection reveal themselves to be empty containers and rhetorically hollow. The case of Mafiaboy is interesting because it yields so little, yet does so on such a grandiose stage. There is much to learn from Mafiaboy's failures.

Why Study Mafiaboy?

11 While Mafiaboy was being excoriated by his peers, his lawyer, Yan Romanowski, was developing a strategy for his defense that reflects core issues in the academic literature on hackers. And it is this issue that warrants critical consideration of the case of Mafiaboy. 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 defense 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 Web sites in question. The defense strategy that emerged in June 2001 was that the accused's motive was "public service" and 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 (opposed to a "black hat" cyber-criminal who hacks with malicious intent) conducting "experiments" that would ultimately help selected Web sites create better security systems. His hacks simply provided proof of security problems and at the same time were giant steps toward providing solutions to such problems; it was a simple trick: expose the fault and then deliver the solution. The point of his experimentation was to land a position as a computer security analyst. Evidence from his appointed social worker, Hanny Chung, was introduced to the court to the effect 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 his stated beliefs. Further evidence indicated that the accused's father had earlier received warnings from the FBI in which it was believed that a computer in his home may have been used for illegal activities in the US; this led to the cancellation of the boy's Internet account, rather than formal charges, due to lack of evidence. Ms Chung also reported that Mafiaboy showed little remorse, a statement hotly disputed by the defense. The effort to fend off the suggestion that the accused serve time in closed Youth Detention was met with the counter-assay of probation and community service, arguing on the basis of the non-violent nature of the actions, and that there was no reason to assume that closed custody would serve any purpose other than exposure to violent offenders, as well as evidence that the youth had learned from his mistakes. Mafiaboy's belief that he hacked in order to test security systems was soundly criticized on technical grounds, including the unnecessary length and intensity of the DDoS attacks (more than poor experimental design, to be sure) at issue as well as repeated refusals to acknowledge posted warnings on software about the illegality of its application to public Web sites.

12 Although the defense was not successful, after all, premeditated criminal intent was proven and Mafiaboy sentenced, and the Judge went out of his way to dismiss as implausible the security test arguments, the effort to shift the debate away from technico-legal evidence, and psycho-social characterizations of the young hacker, onto the political stage warrants serious consideration. The case of Mafiaboy raises the question of the rhetorical limits of hacktivism, that is, the combination of hacking and activism, performed for political purposes, including service perceived to be in the public good. While this issue sits awkwardly with the characterization of Mafiaboy as an adolescent packet monkey aiming 'high bandwidth, low-security [university] networks… like fire-hoses at innocent media giants,' as Poulsen put it, it shifts cyber-crime into the domain of cyber-critique. The politically progressive defense strategy attempted to de-dramatize the narrative of pursuit and capture (the terms of which are outlined by Thomas, 1998: 398-99) typically responsible in media representations for elaborate yet stereotypical characterizations of hackers. Additionally, it sought to defuse the dangerous ligature between technology and the body that in prosecutions and sentencing of hackers has often included a strong element of addiction or "computerholism" (see Duff and Gardiner, 1996: 224 and Thomas, 1998: 396). A. Chandler's (1996:250) study of media representations of hackers in the UK and US notes diverging symbolic economies – the former tending toward criminalization and pathologization, and the latter favouring cowboy and frontier

motifs – but settles on one point: 'the hacker has joined the rogues gallery of modern folk devils.' In Mafiaboy's case, the press repeatedly noted his baggy pants, augmented with loose-fitting jacket, Nike shoes and tees, cigarettes, and backwards baseball cap (the provision of such details have been viciously mocked on 'tribute' sites as tabloid-level reportage). No matter what else he was wearing, Mafiaboy struck a mediatized "gangsta" pose. Socio-semiotically, he was far from appearing as a "white hat" (problem solver) in any sense of the term. His mother went so far as to testify that he stayed up all hours of the night on his computer. His broken family and school troubles were widely documented.

Method and Key Questions

13 In studying the phenomenon of Mafiaboy, I was primarily interested in the media's construction of this hacker in the Canadian context. To this end I gathered several hundred representative samples of journalistic reports (and supporting documents) available from the online editions of mainstream daily newspapers (Toronto Star, National Post, Montréal Gazette, Globe & Mail, Canadian Broadcasting Corporation transcripts from "The National", most of which shared Canadian Press files). Due to fairly high degrees of redundancy among these journalistic sources, I included American reports from a few of the big east coast dailies (Washington Post) and diverse tech publications, as well as "alternative" constructions and assays in the US left-liberal (The Nation) and hacker presses (2600); these latter are important because they constituted direct counter-critiques of the handling of the case as it unfolded. There are thousands of "hits" for a Mafiaboy search on the Web. I selected material on the basis of the new and productive angles, details, and even tangential associations and divergences an item contributed to the overall picture. My basic operating principle was addition and the accumulation of facts and perspectives. The Judge's decision (R. c. M.C. 2001 J.Q. no. 4318) was the yardstick against which I cross-checked facts.

Embedded media, not hosted by this archive: https://journal.fibreculture.org/issue9/genosko1.html

14 ***Figure 1 – Key Dates of the Mafiaboy Case***

Embedded media, not hosted by this archive: https://journal.fibreculture.org/issue9/genosko2.html

15 ***Figure 2 – Other Important Agents and Events***

16 For the sake of clarity I organized two timelines: Major and Minor. (Figures 1 & 2). The former concerned the key dates of the case itself all along the way from the precipitating events to Mafiaboy's sentencing; the latter introduced other important events and agents – statements by notorious hackers, journalists, events concerning Mafiaboy's father, filmmakers, etc.

17 From the outset the US National Infrastructure Protection Center (NIPC) took an intense interest in the case, and information gathered by two key US-based security investigators was passed through the FBI to the RCMP early in the events timeline. The case of Mafiaboy, then, was never only Canadian; rather, it was North American with "global" effects. But the initial flurry of press in mid-February 2000 was attributable to the fact that the leading suspect for American officials was a Canadian (the parochial "Canadian connection" made national English news reports). The NIPC includes Mafiaboy as one of its "Major Investigations." Although the bulk of the material I used was in English, I turned to more recent French sources in order to follow-up the story of Mafiaboy, who had fallen off the media map after his sentencing on September 12, 2001, the day after 9/11. As a personal note, when I attempted to place an op-editorial piece in a national newspaper the day after Mafiaboy's sentencing, I was sternly rebuked by an editor and told that the real news was elsewhere. Circumstances of global proportions have erased Mafiaboy from the media map.

Embedded media, not hosted by this archive: https://journal.fibreculture.org/issue9/genosko3.html

Figure 3 – Content Categories

18 What I created for myself was a media dossier concerning Mafiaboy, which I read for content all along the timeline of events. I am not conducting a content analysis in the traditional sense of attempting to demonstrate trends quantitatively and on this basis make predictions. Much of the material was event sensitive – the breaking story, the arrest, and the sentencing produced reactive

journalistic accounts with small, but significant, variations in how the story was re-presented. In the lull periods I found ideological and technical critiques, and after the dust had settled there was even a cross-media attempt at rebirth. What sort of content was I reading for? My goals were simple. I wanted to understand the construction of Mafiaboy as a hacker and cyber-criminal. I then mapped selected content categories onto the time lines. My two key content categories were "economic impact" and "main suspect attributes." These were augmented by the "other suspects" around Mafiaboy, "security/legal opinions and counter-opinions" and finally "location." (Figure 3) My orientation was backwards-looking rather than protentive-predictive. My analysis of content had the goal of generating contextual markers that would not only focus the analysis but actively prevent it from spilling over into the vast complexity of that moment in informational history. Of course, I do not deny that there were many other shadow markers of context at play around the case. For instance, the deflation of the dot-com bubble after its peak in March 2000 (at least in terms of the rise of the NASDAQ Composite Index) without question intensified the pursuit of Mafiaboy; the United States vs. Microsoft case was beginning to issue findings, media takeovers of gargantuan proportions were occurring, etc. The negative consequence of this strategy of critique is that it stripped the case of Mafiaboy of some of its historical contingency and situatedness, even if one could still say that such contingency stirs in any number of shadow markers.

19 Specifically, I wanted to answer two clusters of questions. First, what sort of hacker was Mafiaboy? This involved journalistic speculation and investigation into and about his personality and skill level. The literature on the construction of hackers as criminals ("crackers") is well-established, and it reveals that such constructions are unstable because characterizations are plagued by historical associations with advanced educational expertise (gifted programmers), counter-cultural activities (Yippie phreaks), and teenage male hijinks (mischief-making), not to mention recent developments in the 1990s that situate hacking as a political practice (see Taylor, 2001) linked to the anti-globalization movement ("hacktivism"). Additionally, around the label "hacker" swirls the relational identity of computer security analysts working against so-called cyber-criminals, but from among whose ranks some of the most notorious have been recruited. This difference has been described as "manufactured" in order to erase the 'uncertainty of the day-to-day exigencies of the IT world' (Taylor, 1999: 116). While hackers may serve as reminders that computer systems are inherently prone to problems and that they must be subject to vigilant surveillance and technical upgrading, there is a 'practical limit to how far this usefulness can be recognized and acted upon outside of a punitive framework' (Taylor, 1999: 117). The enormous similarities between security professionals and hackers are foreclosed by an emphasis on differences, hurried along by the introduction of anti-hacking legislation around the world and stigmatization of the hacker subculture. In one astute Montréal Gazette report, the journalist observed of investigators at the Computer Investigation and Support Unit at RCMP headquarters in Montréal that they 'share traits with the hackers they hunt down' and noted that snapshots of a hacker's room proudly displayed by one investigator 'resembles his own office' (Travers, 2000). Security staff are passionate about computers ('they work at home, in their basements…') while hackers are obsessed with computers. The CISU office itself was said to resemble a 'hacker's lair.' This very passion for computers is a cornerstone of the hacker ethic: "free-rhythmed" creativity and intense sociality because of the strong desire for recognition, despite stereotypes that suggest otherwise (Himamen, 2001: 39 and 52). There are of course rather famous capitalist hackers. The hacker ethic of passion and openness offers an alternative to the "wired cage" of the new economy. Neither hackers nor high-level security analysts are "microserfs" in any sense of this pejorative term (Coupland, 1995).

20 At the same time the hyperbolic criminalization of hackers has been particularly virulent in Canada in recent years as the category of "cyberterrorism" has emerged in strategic studies discourse and circulated through conservative media channels, thereby symbolically uniting the hacker and terrorist. This is one shadow marker that is worth pursuing. What makes the Mafiaboy case so compelling, I am arguing, is that in 1999 then director of the FBI Louis J. Freeh was quoted in the 'Report of the Special Senate Committee on Security and Intelligence,' posted on the Web site of the Canadian Security Intelligence Service (CSIS/SCRS), to the effect that Canada was a 'hacker haven' (CSIS, 1999). In addition, it was rumored that the putative leader of the hacker group Hong Kong Blondes, Blondie Wong, 'is believed to live in Canada' (Bronskill, 1999). This was undoubtedly based on the availability of a Cult of the Dead Cow publication of a dialogue between Blondie Wong (Director, Hong Kong Blondes) and Oxblood Ruffin ('Foreign Minister', cDc) that took place in

a Toronto bar in 1998 and outlined Wong's personal history in Canada (Ruffin, 1998). The dialogue between these two 'Canadians' was largely a political discussion of how hacker cells could help to put back together again human rights and trade policy by exposing and pressuring American corporations doing business in China; indeed, for Ruffin (2004) hacktivism means 'using technology to improve human rights across electronic media.' In the late 1990s the concept of cyber-terrorism circulated widely across several discourses. For my purposes, the most notable feature of this notion was the slippage it created between hacktivism and terrorism. To be sure, in the age of anti-terror legislation the equation has been simplified: hacking+actvitism+cyberspace=terrorism.

21 In 1999 Canadian headlines were screaming 'Now terrorists can strike by e-mail'! (Rose, 1999) At the same time, strategic studies scholars were imagining the next face of war as cyber-biotech terrorism (see the essays in Kushner, 1998). As I mentioned above, there is a definitional slippage that allows for the collapse of hacktivist and terrorist. Two examples are in order. Denning (2000:15) explained that despite bleak prospects for changing policy through the marriage of hacking and activism, hacktivism nonetheless constituted an impressive set of 'operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software.' Her typology included virtual sit-ins and blockades; automated e-mail bombs; Web hacks and computer break-ins; viruses and worms. Cyber-terrorism is defined by Denning as 'politically motivated attacks that cause serious harm' (2000: 24). 'Serious or grave harm' includes severe economic hardship, loss of resources like power or water, injury or death to individuals and groups. The elision of politically motivated hacking as a disruption to normal services and the inclusion of any such services under the rubric of serious harm proved irresistible to some journalists and academics alike (see Rose, 1999; and Stephens, 1998). By contrast, Taylor (2001) emphasizes the factor of 'technological ingenuity' shared by hackers and hacktivists, while embedding the emergence of hacktivism in the history of hacking, simultaneously drawing on established orientations like 'technological curiosity' and the 'deliberate re-appropriation [subversion] of the original purpose of any technology,' with civil disobedience. Taylor writes (2001: 2): 'hackers have become more politically aware and…activists have become more technologically knowledgeable.' The lynchpin is a burgeoning subculture, largely composed of youth but with multi-generational and sectorial tendrils, known as the anti-globalization movement. On the one hand, Mafiaboy's DDoS attacks fit under the general heading of automated e-mail bombs. According to some reports, the serious economic harm he caused was more than a billion dollars US! Hence, by definition, he would be both a hacktivist and a cyberterrorist. He was only once seriously, yet non-specifically, labelled "terrorist" (hackers like him were described as both vandals and terrorists). Moreover, Mafiaboy was also recuperated as an anti-corporate crusader by a leading Canadian journalist aligned with the anti-globalization movement. Taylor (2001) also focuses on the potential of hacktivism to concentrate on an anti-corporate political agenda. Mafiaboy's DDoS attacks on Yahoo, Amazon, Ebay and other e-commerce giants makes him available for inclusion by this political persuasion (Web histories enshrine February 7, 2000 as the day the Net's big names were stopped in their tracks by a Canadian teenager). Ambiguity still exists about what sort of hacker Mafiaboy was since his inclusion under the hacktivist label for his anti-corporate exploits must reckon at some point with the centrist and largely neutral idea of "public service" based on an established point of hacker privilege: understanding and manipulating computer systems, period. But were these hacks nothing but, in the bilious language of Oxblood Ruffin, 'script kiddie antics in [hacktivist] drag'? (Ruffin, 2004) After the fact the RCMP has even come to refer to Mafiaboy as 'unsophisticated' (RCMP, 2002). It is at once both a long way and no distance at all from the figuration of Mafiaboy as cyber-terrorist and public servant. These labels are truly labile. Neither is appropriate, as I will show.

22 Second, what were Mafiaboy's crimes and how should the damage of his actions be assessed? There are general and specific issues at stake here: specifically, monetary estimates about the extent of the damage to potential sales caused by disabling the Web sites of major multinationals, and more generally, the social effects of the acquisition of computer skills. Are hacking skills taught in high school computer classes? Further, if we can understand what kind of hacker Mafiaboy was, it will then be possible to better situate his defense of experimentation toward security employment. Mafiaboy's defense presupposed the evolving relationship between the hacker community and the security sector. The most celebrated may be apprehended, arrested, charged and convicted, but this very process has become more and more readily translatable into

employment in the corporate IT security sector, or at least in terms of expert reportage on it. While Taylor writes of the differences manufactured between hackers and security, Thomas (2002: 87) focuses on the social relations between the two groups within the context of specific operating systems – with UNIX-based systems the relations are "symbiotic" whereas in the case of Microsoft products such relations are based on "extreme hostility." Numerous examples could be cited to make these points. This neither means that a rapprochement between hackers and computer security analysts is taking place nor that the old hard and fast divisions and non-negotiable animosities are being buried. Rather, I prefer another explanation.

23 Mafiaboy may have also discovered the incommensurability of his imagined future as a hacker legend and corporate security employee, and his everyday reality as a computer loving teen whose curiosity passed over into mischief with data, and beyond. The choice of unreality over reality is common to group fantasies among youth subcultures. It's a magical resolution of the contradictions of breaking security systems in order to be welcomed into the computer security fold and of living a dream of peer recognition and celebration, employability and even personal freedom, but alone, before the screen, still a teenager, living with one's parents, in the suburbs. The early studies of Birmingham school cultural studies relating to youth subcultures, especially those of John Clarke et al. (1997), explain the "magical" resolution of the contradiction, by means of subcultural styles and group relations ("lifestyle"), by means of contestation of the dominant culture. Subcultural lifestyles can be quite "unlivable" or what we might say today, unsustainable, even if for a time, late at night, on the weekend, they offer marvelous imaginary, symbolic, solutions to economic exploitation, parental constraints, and vagaries of social mobility, which push reality into the background, at least until Monday morning. Hacking is no different in this respect, and Mafiaboy's wishfulness did not stand up to the youth justice system, to the reality of high school, to the prospects of a McJob. But this was not lost on the Judge. Still, this does not mean that late at night, in his bedroom, before the screen, with his cyber-mates, Mafiaboy had not won for himself a space from the dominant culture (although hackers consider bragging on IRC to be totally "lame"; see Thomas, 2002: 139). 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 duration, but did not play out as a viable answer to the problem of career choice and entry into a profession. Everything in-between was still there.

24 Reading Judge Ouellet's decision in this light makes a great deal of sense. The Judge responded like a seasoned decoder of youth subcultures. He argued, in fact, that his strategy was not to dwell on intent, for there was too much evidence to deny that, but, rather, on motivation. He considered the defense argument that Mafiaboy was only "conducting a test" the results of which would win him a position and/or permit him to develop better firewalls as 'un prétexte ou d'une excuse que d'une réelle motivation.' ['a pretext or an excuse rather than a real motivation'] (R. c. M.C. 2001: para 3). But in the language of the Birmingham school, Judge Ouellet then 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 magicial thinking that, in carrying out what he considered to be an exploit, "un grand coup," his talents would be recognized and this would lead to job offers. But in everyday reality, the real motivation of the accused was to test the 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'] (para 4). The Judge's explanation for Mafiaboy's true motivation was peer recognition and he even goes so far as to state that an experiment would not have required an elaborate network of zombies. Nonetheless, the Judge's reasons for the sentence acknowledge the imaginary solution and the skill required to carry it out.

25

My two key questions (or clusters of questions) are posed within the reasoned framework for a return to the case, that is, the issue of the rhetorical limits of hacktivism, a defense that is stretched to the limits of intelligibility.

Events Analysis

26 One of the most obvious aspects of the Mafiaboy case was that he could not be named under Canadian law (not even the boy's initials, M.C. have entered into circulation, despite the obvious resonance "master of ceremonies" has in rap music culture and for the constructions of Mafiaboy in the fashion sensitive media as a gansta bad boy). In positive terms this meant for hackers that his handle or alias remained front and centre. In hacker culture the handle is privileged and the real name can be dismissed (Thomas, 2002: 132). This question of privilege "calls attention to the act of authorship," Thomas explains (2002: 135) and calls it into question: an author is what a hacker, upon retirement (or arrest), will become, thus claiming for one's own the acts committed under the handle; but while active the hacker remains anonymous, keeping apart online and offline identities. The hacker disappears once a connection between them is made. Mafiaboy retained his handle yet also disappeared; indeed, whether he was a legitimate author in the first place is open to question, at least by his peers. For one of the signs that the hacker underground is dead is, according to Thomas (2002: 139), that it is no longer really underground but accessible to anybody who can buy access to it. Mafiaboy's actions, utilizing DDoS attacks, is a sign of the underground's death and loss of vitality. A further sign is that the trappings of hacktivism can be used as a defense of actions that only offer a post facto justification.

27 In my Minor Events timeline I included the comments of well-known ex-hackers, the two Kevins, Mitnick (2000) (aka Condor) and Poulsen (aka Dark Dante), both of whom are enshrined on 2600′s virtual wall of fame. Both criticized Mafiaboy on technical grounds. But the counterpoint to these criticisms, as well as those leveled by security experts and law officials, was Naomi Klein's posting 'My Mafiaboy' (2000). Klein's posting in the form of a letter to Mafiaboy takes exception to the quick verdicts of Mitnick and others in favour, with tongue in cheek, of another reading: 'At the risk of sounding like a "hacktivism" groupie, let me just say that some of us were able to decipher your encrypted cri de coeur.' Klein's defense of a mythic Mafiaboy who 'hacks in peace' is a masterstroke of political agitation and she is obviously willing to sound like a hacktivism groupie, but in a specific register of her own choice (with requisite mention of classic examples like the 1999 campaign against Etoys that involved Flood Net software and virtual sit-ins; see Grether, 2000). In recasting Mafiaboy as an anti-corporate freedom fighter within the anti-globalization movement, Klein expresses her belief that Mafiaboy was 'committing an act of love…not for the integrity of a particular line of code, but for the Internet in general.' And she also ironized the effect on hackers of the Internet's commercialization: 'In our culture of instant millionaires, computer hacking has evolved into an extreme job application process: Find a weak point in a system, hack it, then offer up your high-priced security services to fix it.' In short, the imaginary solution of a Mafiaboy is an effect of the Internet's commercialization. But Klein's playful justification of Mafiaboy's actions is parodic and an attack on dot.com millionaires and capitalist hackers. Mafiaboy did and did not receive the Klein 'imprimatur': his role was to condense and conduit the ills of a commercialized Internet. My timelines end with the proposal by producer Caroline Héroux, with screenwriter Martine Pagé, for Communications Claude Héroux Plus, of a grant proposal to Téléfilm Canada for a film based on the exploits of Mafiaboy. However, under the terms of Mafiaboy's sentence, he is not to profit in any way – 'directly or indirectly in terms of fame, reputation or financial gain' from his crimes. To date, this proposal did not receive funding.

28 In Figure 3, 'Canada's Mafiaboy,' I deploy five core categories in order to sort the contents of media reports. The most general is 'Location,' which simply indicates the passage from Toronto to Montréal, and from urban to suburban locale. The initial assumption that the ISP was in Toronto was refined as information became available and the focus shifted to Montréal but within the same company. The shift to Montréal was put in stark relief by statements reported in the press about how low, in national terms, computer use was in Québec[1] . All the while the security experts and investigators who came forward with information (correct or otherwise) were all from the US. The combination of Palo Alto expertise (Michael Lyle) and French Canadian locations proved to be a point of some contention when members of hacker quarterly 2600 set out to show that they had spoofed Lyle. As they explain: 'When the name"mafiaboy" was first mentioned

months ago, a couple of us hopped onto IRC using that nick. Sure enough, within seconds, we were being messaged by people who believed we were the person responsible. Amazingly, the person who fell for it the hardest is the very person now being quoted widely in the media as having caught the perpetrator.'[2] The lengthy IRC logs provided by the magazine include a few clues dropped: the use of "oui" and an explanation of why the takedowns were done as something to do on a "snowday." As 2600 explains, 'we were amazed when the blame actually landed on someone from Montréal.' Fiction had become fact. In the absence of verification of the dates of the IRC logs (dated Feb 10), the 2600 spoof rings less loudly (but is a part of the journal's steadfast belief in freedom of expression, that includes denial-of-service attacks as well), but nevertheless makes a clear and essential point about how easy it is to become a suspect – "change a nickname." Indeed, what counts as "credible evidence" is also called into question by 2600 – for them it is fictitious. The 2600 strategy is to force the disclosure of evidence by any means necessary, calling into question the claims of private computer security investigators. That anybody using the handle Mafiaboy was suspect is shown in my reference to a young boy, Mafiaboy2, mistakenly contacted about the case in mid-February and forced to issue a denial. While Lyle was pursuing a certain Mafiaboy, De La Garza (among others) was chasing another suspect, "Coolio." The 17-year old Coolio was contacted by security investigators and FBI agents in early March on the basis of a rumour about his exploits for which he jokingly took credit (AP, 2000). Although other suspects surfaced over the course of events – such as Nachoman and Sinkhole – the supposition that remained even after Mafiaboy's apprehension and arrest was that the attacks of the week of February 7th involved more than one person. Mafiaboy's friends became suspects, and the rhetoric about the "real culprits" waxed and waned according to the degree to which one valorized or criticized Mafiaboy's computer skills. The prevailing belief among security investigators was that amateurs like Mafiaboy are likely "mentored" by more serious criminals, a position published by the RCMP, for example (CP, 2002). As the characterization of Mafiaboy became progressively negative, and his "exploits" firmly recognized as derivative applications, the search for other suspects heated up. To be frank, Mafiaboy would not and could not get any respect.

29 What can be learned from the qualities attributed to Mafiaboy? The overall effect is incoherence and incommensurability of terms. Two emphases are evident: downplaying the technical skill required to carry out the attacks, which occasionally permits a boilerplate description of the criminal whiz kid to slip past. Recourse to stereotypes of the cultural moment is not uncommon in the press. However, a further effect of the repeated use of the Mafiaboy handle was a barrage of soft demographic observations: the smart affluent bored white teen Anglo bad boy from the suburbs. Within these constructions could be found qualifications – that Mafiaboy wasn't a computerholic; that he was self-taught, thus diffusing a potential panic about the uncontrollable effects of computer training in high schools. The distinction that emerged between white hat and black hat hackers – the former seeking system flaws in order to repair them and the latter seeking the same in order to exploit them – compromised Mafiaboy's position when taken in the context of hacker subculture. It is simply not possible for a script kiddie to be counted as a white hat because of the derivative nature of the hacks in question (the title is unearned; Thomas, 2002: 42-4). Perhaps one can only say that Mafiaboy lived the label of white hat imaginatively and communicated this dream to his attorney. By the same token, compared with the low level knowledge of untrained end users (a derogatory term sometimes in the form of 'luser'; see Rose, 2003:58) of computers, Mafiaboy did possess arcane and detailed technical expertise, yet this would not have had currency in the hacker subculture where 'hackers make their reputations by releasing these bugs and holes in basic "security advisories", by publishing them in hacker journals, by posting them online at places like The L0pht... or by publishing them on mailing lists such as Bugtraq...' (Thomas, 2002: 44-5).

30 The question of spectacular and hyperbolic assessments of the economic damage caused by Mafiaboy's DDoS attacks warrants a final note. Estimates of losses are just that – estimates arrived at by speculation and extrapolation: revenue losses, losses in market capitalization, costs for upgrading security holes, and repairing consumer confidence. These are potential losses rather than real losses or damages. The movement from millions through hundreds of millions to billions was never justified nor explained. Certain impressive numbers were produced by third parties like the Boston Yankee Group but they lacked foundation. The big numbers were consonant with the shock of the new (not the first DDoS attack but the first big wave against established names) and

the space they grabbed as the major events unfolded in a highly charged atmosphere of highs and lows. But the big numbers did not enhance Mafiaboy's reputation among his peers. The big numbers did, however, attract a united North American intelligence response.

Concluding Remarks

31 Ultimately, the Judge did not accept Mafiaboy's explanation of why he hacked. Indeed, his peers were not impressed, either, and would not accord him the status of white hat. But Judge Ouellet did not balk at utilizing Mafiaboy's interest in computers as a way to deal with the issue of recidivism. He rejected draconian suggestions by the Crown and social worker that Mafiaboy not be permitted to visit the Web sites he attacked and even use a computer for a certain period. Judge Ouellet turned the boy's attention in the direction of finding more interesting and constructive challenges, such as gaining proficiency in multiple computer program languages. The end point was to have Mafiaboy himself discover this: 's'il parvient à acquérir la maîtrise de différents langages de programmation ainsi que la capacité d'utiliser et /ou de créer des logiciels d'avant garde, il pourra alors réaliser que ce qu'il considérait (et considère possiblement encore) comme un tour de force, n'était en fait qu'une action qui, bien que nécessitant des connaissances et des habiletés peu usuelles chez un adolescent de 15 ans, demeure à la portée de beaucoup de gens possedant des connaissances de base du fonctionnement des réseaux informatiques.' ['if he can learn to master different program languages as well as the ability to work with and/or develop innovative software programs, he might then realize that what he considered (and may possibly still consider) a tour de force, in fact was only an action which, though requiring knowledge and technical skills not commonly possessed by 15-year olds, is within the scope of many people with basic knowledge of information networks'] (para 14). By focussing Mafiaboy on the question of the knowledge requirements for the real, lived passage from precocious 15-year old to skilled programmer, Judge Ouellet encouraged him to make use of his longstanding interests and talents. For the Judge, then, Mafiaboy did not hack in peace with a view to the public good; only "mythically" and "magically" was he a white hat. This decision was also reached in the hacker subculture proper, with the exception that the case itself illustrated the depths to which the underground had been dragged.

32 What makes the case of Mafiaboy valuable are the limits of the hacktivist justification; a good example of a bad usage. The defense arguments that Mafiaboy hacked in the "public service" broke down into a kind of imagined self-interest towards the goal of finding solutions to security flaws on storied ecommerce Web sites; they are rendered incoherent when taken together with the abilities of a script kiddie. Mafiaboy was not producing tools in the public or private service; he was not mounting a critique of global capitalism with a mass action; he was not freeing access and thus empowering Web surfers. At the same time he was not exploiting system holes for profit; neither was he damaging software nor hardware. His crimes were "temporal" in that he denied access to Websites for a certain time. Judge Ouellet even notes (para 7) that the big numbers posted as potential losses were not pursued by the vendors as damages – not one corporation came forward before the court to seek damages and it is this lack of cooperation that concerns him, especially in light of the phantasmagoria of media speculation about the case. This opinion has, I believe, oriented the RCMP toward building better contacts with ISPs, the tendency of which is not to report incidents of hacking but simply to quietly close accounts. The Mafiaboy case is cited as primary example of the need for a winning strategy (RCMP, 2002) 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.'

33 Mafiaboy's motives were "private" in as much as they concerned his own career, and his means were not very elegant and traceless. These latter considerations ran him afoul of the "digitally correct," that is, those who would dismiss any DDoS attack on the basis of its lack of sophistication (Jordan and Taylor, 2004: 90ff). This position would a priori exclude even those well-respected political mass actions by means of Flood Net software undertaken by the Zapatistas (Taylor, 2001). Mafiaboy's attacks were hardly MIT calibre pranks, either (Peterson, 2003). But Jordan and Taylor (2004: 77-79) contrast digital correctness with mass action hacktivism.

34 DDoS attacks are primary examples of mass action hacktivism. However, they are only part of the story, as Jordan and Taylor explain. Refining our understanding of "distributed," the authors split

this category into two: on the one hand, automated, server side operations by means of distributed zombies under centralized control; and, on the other hand, client-side, non-server concentrated, coordinated attacks by tens of thousands of individual computer users (all of whom have downloaded software at a particular site with a few clicks). One important difference between automated and client-side DDoS attacks is that the former requires a much higher level of technical skill than the minimal skills required by the latter (indeed, in this instance all sorts of hardware and connections are being used, some not very up to date and slow). This makes client-side DDoS inefficient, but mass, whereas the automated, Mafiaboy-type attacks require a higher level, but not ultimately, a sufficiently high level of technical ability to garner respect. Only the mass client-side attack has "ethical" status because it is seen as a genuinely activist response, such as the Electrohippies Collective action against the World Trade Organization's Web site during the anti-globalization protests in Seattle in 1999 (Jordan and Taylor, 2004: 77).

35 In the end, the case of Mafiaboy reveals the rhetorical limits of hacktivism as a defense for an automated DDoS attack, yet does not disqualify him from hacker status for, after all, as almost everyone involved acknowledged in one way or another, to hack is to believe, at the simplest, in one's action, and this is an 'idealization' (Jordan and Taylor, 2004: 9) often lived virtually. Yet if this means that the critical distinctions that define the hacker underground are open to widespread abuse and appear empty, at least in the case of Mafiaboy, what does this say about the underground's ability to control its own boundaries? That hacker notables denounced Mafiaboy's actions, parodied and even baited security analysts, shows us that the subculture has its border rangers but is fighting a difficult battle to win back its means of identity formation and control the terms of membership. That some of its key defenders are now on the other side, having passed through magical thinking and into security analysis and expert technical reportage, some via prison, suggests that legitimation has its burdens, that is, the burden to try and exclude from the ranks those who pretend to the code of belonging, even if parts of the code have become fuzzy in the process and are now available to all those who would like to try them on for size. Under these conditions the time, energy and collective willpower required to expose a poseur places an enormous burden on the ranks and resources of hacker subcultural groups.

Acknowledgements

I am grateful for the assistance of Scott Thompson, research assistant in my Technoculture Lab, for his work on the Matrix-style figures accompanying this article. We thank the Canada Foundation for Innovation, the Canada Research Chairs program of the Social Sciences and Humanities Research Council of Canada, and Lakehead University, for their ongoing support. I would also like to thank Dr. Paul A. Taylor (Leeds University), as well as the anonymous reviewers of this manuscript, for their helpful comments.

Author's Biography

Gary Genosko is Canada Research Chair in Technoculture at Lakehead University in Thunder Bay, Canada. His recent work has focused on the intersections of administrative technology, race, and alcohol in historical context. He is currently working on 'Phreaking the Maple Leaf' – Canadian hackers, phreakers, and anti-surveillance cyborgs.

Notes

[1] Is there anything to be learned from the newspaper wag who pointed out the irony that Mafiaboy was operating in Québec, one of the provinces where Internet use lags far behind Canadian usage rates? Couldn't the opposite be asserted – that an "underdeveloped" location provides greater opportunities given lax governance of ISPs and weak industry oversight mechanisms, for rogue elements to operate successfully over a greater period of time? Neither hypothesis is very satisfying, to be sure. But that doesn't change the obvious. From 1999-2003, Québec households lagged well behind the Canadian average in every category of sites from which the Internet is accessed, according to Stats Can, and was second last overall (in front of New Brunswick) with regard to any location (home;work;school;public library;other), and third last in access from home (in front of Newfoundland and Labrador and New Brunswick) (2005). Perhaps these matters are less relevant than the metropolitan figures. Montréal exceeded the Québec average for access from any location (58.7% of households as compared with 54.9%), but was

below the provincial figure for access from home (48% – 44.5% in 2003). Both these numbers rank far below Canadian figures for the same year (all locations 64.2% and home access 54.5%). One would be wise to look for two factors at work: the failure of ISPs to reach the mass home market, and cultural ambivalence toward home Internet access, as well as rates of computer ownership with or without such access, not to mention demographic issues, dense and sparse clusters of access around university centres, etc. (Statistics Canada, 2003)

[back]

[2] See the provocation 'Is Mafiaboy Real or a Creation of the Media?', https://www.2600.com/news/view/article/327

[back]

References

Aarseth, Espen J. Cybertext: Perspectives on Ergodic Literature (Baltimore: The Johns Hopkins University Press, 1997).

AP. 'Young hacker won't take redit for attack', The Globe & Mail (March 4, 2000).

Bronskill, Jim. '"Hacktivists' and cyber-outlaws growing threat: CSIS', The National Post (June 26, 1999).

Canadian Security Intelligence Service. 'Cyber-terrorism' (1999), https://www.csis-scrs.gc.ca/eng/operat/io2e.html

Chandler, Amanda. 'The Changing Definition and Image of Hackers in Popular Discourse', International Journal of the Sociology of Law 24 (1996): 229-51.

Chandler, Jennifer. 'Security in Cyberspace: Combatting Distributed Denial of Service Attacks', University of Ottawa Law & Technology Journal 1 (2003-4): 231-61.

Clarke, John and Hall, Stuart and Jefferson, Tony and Roberts, Brian. 'Subcultures, Cultures, and Class' in The Subcultures Reader ed. Ken Gelder and Sarah Thornton (New York: Routledge, 1997; 1975), pp. 100-11.

Coupland, Douglas. Microserfs (Toronto: HarperCollins, 1995).

CP. 'Amateur hackers huge security threat: RCMP', The Thunder Bay Chronicle-Journal (March 9, 2002).

Denning, Dorothy E. 'Activism, Hacktivism, and Cyber-terrorism: The Internet as a Tool for Influencing Foreign Policy', IWS-The Information War Site (2000), https://www.iwar.org.uk/cyberterror/resources/denning.htm

Duff, Liz and Gardiner, Simon. 'Computer Crime in the Global Village: Strategies for Control and Regulation – in Defence of the Hacker', International Journal of the Sociology of Law 24 (1996): 211-228.

Greenberg, Lee. 'Swedish whiz kid helps FBI track virus', The National Post (May 12, 2000).

Grether, Reinhold. 'How the Etoy campaign was won', Telepolis (Feb. 26, 2000), https://www.heise.de/tp/english/inhalt/te/5843/1.html

Himanen, Pekka. The Hacker Ethic and the Spirit of the Information Age (New York: Random House, 2001).

Klein, Naomi. 'My Mafiaboy', The Nation (March 13, 2000), https://www.thenation.com/doc/20000313/klein

Jordan, Tim and Taylor, Paul A. Hacktivism and Cyberwars: Rebels with a Cause? (London: Taylor & Francis, 2004).

Kushner, Harvey W. (ed.) The Future of Terrorism: Violence in the New Millennium (Thousand Oaks: Sage, 1998).

Mafiaboy [2600 Staff] and Icee. 'Is Mafiaboy Real or a Creation of the Media?', posted 20 April 2000, https://www.2600.com/news/view/article/327

McTaggart, Craig. 'A Layered Approach to Internet Legal Analysis', McGill Law Journal 48 (2003): 571-625.

Mitnick, Kevin. 'Opinion: Convicted Hacker Kevin Mitnick', (Feb 13, 2000), https://www.time.com/time/pr/mitnick.html

Ouellet, Gilles L. La Reine entre M.C. J.Q. no 4318 (12 Sept, 2001, 27 paras).

Peterson, T.F. Nightwork: A History of Hacks and Pranks at MIT (Cambrdige: MIT Press, 2003).

Poulsen, Kevin. 'Free Mafiaboy', (April 24, 2000), https://www.securityfocus.com/news/22

—. 'Rise of the Spam Zombies', (April 25, 2003), https://www.securityfocus.com/news4217

Royal Canadian Mounted Police Criminal Analysis Branch. 'Hackers: A Canadian Police Perspective, Part 1′ (2002), https://www.rcmp.ca/crimint/hackers_e.htm

Rose, Alexander. 'Terror has a New Name: The Internet', The National Post (July 3, 1999).

Rose, Ellen. User Error: Resisting Computer Culture (Toronto: Between the Lines, 2003).

Ruffin, Oxblood. 'Hacktivism, From Here to There', (28 March, 2004, Yale Law School), https://www.cultdeadcow.com/cDc_files/cDc-0384.html

—. 'The Longer March: Interview with Blondie Wong', cDc communications #356 (July 15, 1998), https://www.cultdeadcow.com/cDc_files/cDc-0356.html

Schwartz, John and Cha, Ariana Eunjung. 'Clinton Pledges Support at Anti-Hacking Summit', The Washington Post (Feb. 16, 2000).

Statistics Canada. CANSIM, Table 358-0002, 2003, modified 2005.

Stephens, Ralph Eugene. 'Cyber-Biotech Terrorism: Going High Tech in the 21st Century' in H.W. Kushner (ed.) The Future of Terrorism: Violence in the New Millennium (Thousand Oaks: Sage, 1998), pp. 195-207.

Taylor, Paul A. 'Editorial: Hacktivism', The Semiotic Review of Books 12.1 (2001): 1-3.

—. Hackers: Crime in the digital underground, London: Routledge, 1999.

Thomas, Douglas. Hacker Culture (Minneapolis: University of Minnesota Press, 2002).

—. 'Criminality on the Electronic Frontier: Corporality and the Judicial Construction of the Hacker', Information, Communication & Society 1/4 (1998): 382-400.

Today in Technological History. 'February 7′, The Center for the Study of Technology and Society (2002), https://www.tecsoc.org/pubs/history/2002/feb7.htm

Travers, Eileen. 'From top cops to computer nerds', Montreal Gazette (April 20, 2000).

Turkle, Sherry. The Second Self: Computers and the Human Spirit (New York: Simon and Schuster, 1984).

Vise, David and Cha, Ariana Eunjung.'Canadian Teen Charged in Web Blitz', The Washington Post (April 20, 2000).

The Fibreculture Journal (ISSN 1449-1443) — Issue 9, 2006-12-05. This article is published under CC BY-NC-ND. The author retains copyright.

This PDF is an archival offprint generated from the journal's text archive on 2026-11-15. It is not the publisher's version of record; the published article is at https://nine.fibreculturejournal.org/fcj-057/. Page numbers here are not the published pagination. Where paragraph numbers appear in the margin they are the journal's own and are the citable unit.