

GOVERNMENTALITY AND THE WAR ON TERROR: FBI PROJECT CARNIVORE AND THE DIFFUSION OF DISCIPLINARY POWER

HOLLY E. VENTURA, J. MITCHELL MILLER and
MATHIEU DEFLEM

University of South Carolina

Abstract. Social control capabilities have increased significantly over the past several decades, particularly because of an increased utilization of technologically advanced surveillance methods. Following the tragic events of September 11, 2001, U.S. Congress and the present Administration have granted law enforcement considerable new powers in the enforcement and prevention of terrorism-related crime. Collectively labeled under the heading of the so-called “war on terror”, the scope of such laws, policies and directives are challenged by civil rights organizations and numerous legislators for lack of definitional precision, arbitrary application of sanctions, and violation of privacy laws. One of federal law enforcement’s surveillance tools is “Project Carnivore,” a Justice Department Internet surveillance program that is administered by the Federal Bureau of Investigation (FBI) to access information flowing to and from a central processing unit on a network connection. While, theoretically relying on Michel Foucault’s theory of discipline and governmentality, as well as related insights in the social control literature, this paper examines Project Carnivore relative to the larger context of state rationality and related privacy issues.

Introduction

Throughout United States history, practices and institutions of social control have always sought to maintain a proper balance between the individual rights of citizens and what is commonly referred to as “national security.” The challenge of maintaining this balance has never been more pronounced than since the events of September 11, 2001 and the subsequent onset of the so-called ‘war on terror.’ Criticized by civil rights groups and legislators from both sides of the aisle for lack of precision in defining the term ‘terror’ and an arbitrary application of vague standards for detention and sanctioning, this new conflict poses many critical criminological issues that can have far-reaching implications for the future of our criminal justice system. Many opponents consider the war on terror to be an attack on the Fourth

Amendment of the U.S. Constitution, while others point to more general concerns characterized by references to the “Big Brother” concept and governmental omnipotence, which have been fairly common in the popular discourse on terrorism (Birdis 2001; Lerner 2003; Voors 2003).

Far more than a mere formulaic catch-phrase, the war on terror consists of an extensive number of laws, policies, and directives aimed at preventing additional attacks on, primarily, American targets. Legislation and executive directives alike carry significant implications for the function of law enforcement, particularly with respect to privacy issues. Several initiatives included under the broad umbrella of the terror war teeter dangerously on the fringes of constitutionality, theoretically presenting a legal and ethical quagmire for the government. A primary example is the USA Patriot Act, legislation passed by Congress six weeks after the September 11th attacks, which broadened government’s surveillance powers in several areas including records searches and intelligence searches. In this paper, we focus on one specific initiative, a new technology developed for the Federal Bureau of Investigation (FBI), termed “Project Carnivore.” Despite selective implementation prior to September 11, it is particularly since that fateful day in our nation’s history that Project Carnivore may have great implications for the nation’s latest national security endeavor as well as with respect to the rights of individuals who have access to targeted Internet Service Providers.

Perhaps the most intrusive web-based technology ever developed, Carnivore possesses the ability to essentially wiretap individuals’ computers, accessing every piece of datum flowing to and from a Central Processing Unit (CPU), provided the data were moved on a network connection. But Carnivore opens up a privacy ‘can of worms,’ as the technology far out-paces present laws aimed at the protection of individual liberty and privacy. And, indeed, the surveillance project has already been examined on a number of grounds, including possible Fourth and First Amendment abuses and violation of the Electronic Communications Privacy Act (ECPA) of 1986. Yet, although several groups have expressed a desire to challenge the project’s constitutionality, the ECPA at present remains the sole source of judicial action concerning Carnivore (American Civil Liberties Union (ACLU) 2002, 2003; Gooldstein and Orr 2003; StopCarnivoreNow 2003).

The Electronic Privacy Information Center (EPIC) filed a complaint against the U.S. Department of Justice and the FBI in Federal District Court (Civil Action No. 00-1849 JR) in 2000 for failure to comply with the Freedom of Information Act (FOIA). Despite numerous requests,

the Bureau initially refused to provide the EPIC (a non-profit organization aimed at the educational dissemination of privacy-related policies) with documents related to the nature and utilization of the Carnivore software based on a national security argument. Upon further demands from the EPIC, the FBI then released 1957 pages of material, but some pages were edited, visually obstructed, or missing. The EPIC continued its quest for Carnivore-related documents and a federal district judge in Washington, D.C. ordered the FBI to identify the location of all possible material related to the Carnivore software system. The Bureau now asserts that all documents related to the software have been made available in compliance with the FOIA. The FBI's initial claim of national security protection coupled with its subsequent refusal to produce documents in their totality exemplifies the difficulty with which the legal community is faced in understanding and assessing the nature and scope of the Carnivore program. Moreover, the judicial climate today is such that executive agencies are not held to a strict definition of national security, thus creating the problem of lessened accountability in terms of FOIA compliance.

Research on social control has focused on the escalation and intensification of surveillance monitoring from social-scientific (Cohen 1985; Marx 1988), cultural (Marx 1997, 2002), historical-comparative (Deflem 1997; Foucault 1977), and ethical (Foucault 1980; Lerner 2003; Marx 1998) viewpoints. The nature of Carnivore's sweeping capabilities hastens questions of government intention and specification of latent and manifest functions of the program. In this paper, we will examine the legality and ethicality of Project Carnivore in the broader context of a Foucauldian perspective of governmentality and state rationality (Foucault 1980, 1991). Before addressing the implications and possible consequences of an unbridled use of Carnivore, we briefly describe the Project and its technical components.

FBI Project Carnivore

What exactly is Project Carnivore? It is important to precisely define the Carnivore program to avoid getting entangled in a discussion of its ethicality and public policy implications that is not rationally grounded. Project Carnivore is part of a third generation of online-detection software programs used by the FBI and is a part of a larger more comprehensive system, the Dragonware Suite, which allows the Bureau to reconstruct email messages, downloaded files or even web pages

(Tyson 2003). Although the FBI has provided minimal information to the public about the Dragonware Suite, and little detailed information regarding Carnivore, the system is basically what is referred to in computer terms as a 'packet sniffer.' A relatively common technology that has been available since early 2000, a packet sniffer is a program that can see all of the information on a specific network, examining or 'sniffing' packets of data streams. The software is capable of reconstructing any web pages, web-based text documents, and the contents of email messages. Thus, as a mechanism of social control, Project Carnivore operates primarily as a means of offender and offense identification (Marx 2002).

Who does Carnivore target? According to the FBI (2000a), Project Carnivore will only be utilized by the agency when a group or person is suspected of terrorism, child pornography or exploitation, espionage, information warfare or fraud. The Bureau denies the ability to engage the software at whim, noting that the use of Carnivore is controlled under Title III of the Electronic Communications Privacy Act, which provides legal protection of privacy for all types of electronic communication. Therefore, the Bureau is required to obtain a court order to utilize the tool. Unlike search warrants that are needed to search houses or other physical property, applications made under Title III for intercepting wire and electronic communications require the authorization of a 'high level' official from the Department of Justice before a local United States Attorney office can make an application to a federal court. The term 'high-level' official, however, is not precisely defined. Also, unlike typical search warrants, federal magistrates are not authorized to approve such applications, which instead are reviewed by federal district court judges. Additionally, interception of communications is limited to the aforementioned federal felony offenses.

Applications for the use of Project Carnivore must indicate that other, ordinary investigative law enforcement techniques have been attempted but failed to gather evidence of a crime, or will not work or are considered to be too dangerous. Also included must be information concerning any prior electronic surveillance regarding the subject or facility in question (FBI 2000a). Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if investigation objectives are met. It is within a judge's discretion to require periodic progress reports advising the court of the interception effort. Like court-ordered telephone wiretaps, interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as

unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application (FBI 2000a).

Project Carnivore is constructed by the FBI, then, as being no different from and no more problematic than any other investigative technique utilized by law enforcement to thwart the threat of terrorism and protect society. The software is also contended to be safe from any abuse, because the program cannot be executed unless it has been approved under the watchful eye of a federal district court judge. But this system of juridical review need not always be relied upon. "Of course," the FBI acknowledges, "there are 'emergency' provisions whereby surveillance is permitted to proceed immediately, when high-level Department of Justice authorization is obtained, so long as a court order is filed within 48 hours" (FBI 2000b). To date, the Bureau has not offered any explication or instances of this emergency provision.

Questioning the Constitutionality of Carnivore

Critics have argued that use of the Carnivore software package may violate Constitutional provisions of the Fourth Amendment (ACLU 2002a, b; Birdis 2001; Lerner 2003; Stanley and Steinhardt 2003). Civil rights organizations such as the ACLU protest the use of the tool, arguing that the program is inherently unconstitutional. Other groups likewise make a case for the software's unconstitutionality, but they characterize it as a violation of the First Amendment right of free speech (StopCarnivoreNow 2003). Both views may well form a basis for future legal challenge, but, to date, only the Electronic Privacy Information Center has instigated legal action against the FBI.

The Fourth Amendment Argument

The Fourth Amendment of the U.S. Constitution ensures Americans the right to be secure in their persons, houses, papers, and effects, against any unreasonable searches and seizures. As such, the Fourth Amendment may also apply to the government-regulated monitoring of internet activity (ACLU 2002a, b; Stanley and Steinhardt 2003). What is, and arguably should be, of special concern to those advocating the Fourth Amendment argument against Carnivore is the FBI's caveat that under special circumstances emergency use of Carnivore is allowable for up to 48 hours *sans* court order. This special provision, indeed, appears to be in violation of the Fourth Amendment, as debate

can center on the definition of what is an ‘emergency’ and thus to be judged as reasonable within the confines of the Constitution.

Also of concern is the finding from a report by the Illinois Institute of Technology Research Institute, which was contracted by the Department of Justice to evaluate the Carnivore software, that indicates that when improperly configured, Carnivore is able to record all monitored information (IIT Research Institute 2000). The report concluded that while Carnivore can perform fine-tuned searches for only those data that were authorized by a court order, if the system is “[i]ncorrectly configured, Carnivore can record any traffic it monitors.” Technical glitches in the software can thus contribute to potential privacy violations.

The First Amendment Argument

Through Project Carnivore, information might be obtained that is specific to certain websites for purposes other than national security. For example, according to the Electronic Frontier Foundation (2003), the federal government has utilized Carnivore to entirely shut down some websites and to remove certain information from other sites, in violation of the Freedom of Information Act¹. According to federal law enforcement, these websites were shut down for a range of reasons, including support of terrorism, anti-American sentiment, and violations of the Controlled Substance Act. The Electronic Frontier Foundation has also alleged that other governments have done the same, as have some Internet Service Providers (ISPs). Overall, freedom of speech advocacy groups interpret Project Carnivore as a crucial ingredient in a recipe to suppress Americans’ First Amendment right, which could constitute another step in a slippery slope of tyranny in the name of national security.

Privacy Litigation Against Carnivore

The Electronic Communication Privacy Act addresses the surveillance of electronic communication by the government and specifically considers the use of so-called ‘pen register’ and ‘trap-and-trace’ devices. Pen registers record and decode all numbers dialed by an electronic device (i.e., telephone), while the trap-and-traces capture the originating source of incoming calls. Together, these are commonly referred to in law enforcement jargon as a ‘Dialed Number Recorder’ or ‘DNR.’

Project Carnivore effectively combines the capacities of pen register and trap-and-trace devices. An obvious difference between a DNR and Carnivore is the target of recorded information, as DNR is used on out-going and in-coming phone calls, whereas Project Carnivore monitors sent and received emails and web-browsing destinations.

The sole court action addressing Project Carnivore has challenged its legality on grounds of violation of the ECPA. Internet service provider Earthlink filed a complaint against the Department of Justice in 2000 for ordering the company to allow the FBI to install Carnivore software on Earthlink's network. The company questioned the Justice Department's legal authority under the pen register statute to force the installation. The court determined that although the Justice Department's order was not specifically for a telephone, the use of Carnivore to monitor computer communication did legally equate with the intent of the federal statutes concerning pen register (18 U.S.C. § 3127[3]) and trap-and-trace (18 U.S.C. § 3127[4]). This decision speaks directly to the Fourth Amendment argument in that the court found the government to be within the bounds of legal search and seizure per the ECPA statutes. Until further appeal of the Earthlink decision to a higher court or similar action by the government is contested by other ISPs, Carnivore remains an available surveillance tool.

In sum, much like many other modern mechanisms of social control (e.g., on the prisons, see Foucault 1977), Project Carnivore constitutes a case of purposive action that comes with several unanticipated or unintended consequences (Merton 1936). Primarily, the Carnivore software is intentionally designed as a means to identify an offender or offense. Sociologist Gary Marx (2002) has described the function and relevance of identification as a technique of social control through engineering, by suggesting that absent the power of social control to remove, devalue, insulate, incapacitate, or exclude the offender or offense, it is still possible and valuable for social control to gather knowledge about an actual or potential offense or offender. The Carnivore program, indeed, enables federal law enforcement to gather electronic information in the course of a criminal investigation, specifically data transmitted over the Internet.

Though capable of performing finely-tuned searches where only relevant information is isolated and intercepted, Carnivore might also pose an unintended but very real danger in that the software has the ability to execute overly sweeping indiscriminate inquiries. As the Electronic Frontier Foundation (2000) has argued before Congress,

because the FBI's use of Carnivore has little public oversight, the existence of an overly broad surveillance system by federal law enforcement has the potential to lower people's expectations of privacy as they use the Internet. The potential for privacy abuses is perhaps the gravest of Carnivore's unanticipated consequences.

Social Control Technologies and the Culture of Governmentality

Although criminologists have recently paid more attention to terrorism and terrorism related-topics (e.g., Deflem 2004), they have generally not yet sufficiently addressed the specific programs and strategies that form part of the response to terrorism at the level of government, law, and law enforcement. Project Carnivore, in particular, has received only minimal coverage in criminology as well as other disciplines, such as computer science and economics. To date, relating to the constitutional considerations from civil libertarians, only scholars of law have devoted attention to Carnivore from an intellectual viewpoint. Although some members of the legal community have argued in favor of the use of Carnivore (Dunham 2002; Strauss 2002), most legal scholars agree that Carnivore has the potential to intrude on the civil liberties of Americans in cyberspace (Gilman 2001; Haas 2001; Holmes 2001; Mer 2001; Tountas 2003).

From a more analytically informed perspective, we argue, the Carnivore program presents an instance of the evolving rationality of social control that Michel Foucault (1977, 1981, 1991) has described as governmentality. In *Discipline and Punish* (1977), Foucault developed the theory that the disciplinary effects of power, which had originally been developed in prison, gradually spread throughout society in all kinds of manifestations aimed at correcting and normalizing individuals. Aimed at producing docile bodies in a society's population, disciplinary power moves beyond the walls of the prison "right down into the depths of society, . . . down to the finest grain of the social body" (Foucault 1977: 27, 80). Thus, discipline steadily grows and expands to become a "whole complex mechanism, embracing the development of production, the increase in wealth, a higher juridical and moral value placed on property relations, stricter methods of surveillance, a tighter portioning of the population, more efficient techniques of locating and obtaining information" (77).

The perspective of governmentality explains the diffusion of disciplinary power as the result of a transformation of power from a nega-

tively oriented concept (to forbid) towards a positive notion of power that centers on the members of a population in all aspects of their behavior (Deflem 1997; Foucault 1980, 1981, 1991; Gordon 1991). Dating back to political thought of the 16th century, governmental power extends to the current phase of neo-liberal mechanisms of social control by centering on each and every thought and action of any and all people as the building blocks of law and order. Social control is not merely crime control (literally: the control of criminals), but extends to an entire population and its potential relevance to positively or negatively affect the security of the nation. Thus, a whole series of knowledge systems is developed (e.g., traditional criminology as criminal justice administration) and a sophisticated apparatus of strategies and tools is devised and implemented to foster the development of this power-knowledge.

Although Foucault's research of power was centered on discipline in correctional contexts, his discussion also provides an adequate framework in which to consider Project Carnivore. For, indeed, as other scholars discussing practices of social control in advanced capitalist societies have observed (Baddeley 1997; Garland 1997; Walters 2003), the governmental diffusion of disciplinary power continues to characterize modern systems of social control. At the most general level, as a system of deeply penetrating surveillance, Carnivore represents a means of correct training which Foucault (1977: 170–194) describes as an 'examination,' i.e., a method of disciplinary power that is able to see and record every move and thought of each and all, but that itself cannot be seen. Resembling the ever-present powers of the central watchtower in a prison modeled after the Panopticon, the very fact that the FBI has the potential to monitor communications on a website may lead Internet users to believe that they are constantly being watched. The proven fact that there have been crimes that were perpetuated by reliance on the internet (e.g., the September 11 hijackers planned their attacks via email) justifies the federal law enforcement response to target the internet.

Besides the fact that the enacted system of surveillance may go well beyond its initial justification, the very development and utilization of the Carnivore software has effectively enabled law enforcement to further increase its arsenal of disciplinary tools. It is important in this respect to note that Project Carnivore was initiated by the FBI more than a year prior to the terrorist attacks of September 11. Although it may be relatively easy to accept the need for the software since the events of 9–11, especially given the fact that the hijackers orchestrated

the attacks via the internet, it is more difficult to reconcile that federal law enforcement planned on utilizing this technology prior to the current state of emergency.

According to Foucault (1980), disciplinary power creates “a machine in which everyone is caught” in order to accomplish a system of “total and circulating mistrust” (156, 158). In this context, it is difficult to accept at face-value that social control is a mere functional response to crime. In the case of Project Carnivore, high-level Bureau officials have linked the system intimately to the investigation of criminals. For example, John E. Collingwood, the Assistant Director of the Office of Public and Congressional Affairs of the FBI, defended Carnivore by simply stating that the software would be used to “to obtain a criminal’s e-mail. . .” (Collingwood 2000b). In a theoretical vacuum, the use of the word ‘criminal’ is powerful, but misleading and somewhat at odds with the notion of an adversarial and due-process orientation to law and justice. A central tenet of the criminal justice system in our society is the presumption of innocence. Labeling the targets of criminal investigations prematurely as ‘criminals’ compromises the spirit of the justice process. Ironically, also, the constitutive effect of the labeling might imply that all those who are monitored will be considered criminals, because the logic of an official investigation is based on the premise that only criminals will be monitored.

The FBI’s position on the Carnivore software, the published official statements regarding the project, and the very name of the Project all suggest a culture in the ranks of social control agents that advocates a ‘by-any-means-necessary’ mindset that fits well with the totalizing aspirations of disciplinary power. The enthusiastic atmosphere among law enforcement circles surrounding the Carnivore program thus demonstrates the value of a Foucauldian emphasis on the mechanisms of power beyond the confines of formal legality (Foucault 1980, 1981). Thus, the Carnivore software affords the FBI powers extending far beyond law enforcement’s previous ability to obtain information regarding possible criminal behavior under the provisions of the so-called Katz decision. Citing that persons had a reasonable expectation of privacy, not an absolute one, the Katz decision authorized only the specific system of telephone wiretapping (*United States v. Katz* 1967). But since the arrival of Project Carnivore, law enforcement is able to tap into virtually any medium of communication, save for face-to-face conversations between persons who are not under electronic surveillance. Although the FBI asserts that only specified materials would be monitored by Carnivore, the IIT Research Institute’s (IITRI

2000) independent evaluation of the software states that the system “is also capable of broad sweeps” (xiii). Carnivore thus might well realize the ideal of disciplinary power to extend beyond the prison walls and move “through progressively finer channels, gaining access to individuals themselves, to their bodies, their gestures and all their daily actions” (Foucault 1980: 152).

The Ethics of Carnivore

Project Carnivore is being questioned by a variety of sources, ranging from the media to civil liberties groups and politicians (ACLU 2002a, b; Electronic Frontier Foundation 2003; Scheeres 2001; Stanley and Steinhardt 2003; Vlahos 2001). Although criticisms generally center on the central ethical issue of the potential of Carnivore to violate privacy rights (Holmes 2001), various more specific arguments can be mentioned that expose the potential problems with Carnivore.

First, findings from the report by the Illinois Institute of Technology Research Institute indicate that Carnivore can be accessed by a username/password combination, making the system vulnerable to potential hacker abuse (IIT Research Institute 2000). As there is no way to trace the source of Carnivore software operation, computer experts have the opportunity to hack into Carnivore and perhaps install it on an ISP, all with little chance of detection and prosecution. This problem is commonly referred to as the ‘backdoor problem’ (ACLU 2002, 2003; Electronic Frontier Foundation 2003; StopCarnivoreNow 2003). Personal spying, accessing computers, shutting down websites, passing computer viruses and halting e-mail traffic are all potential ramifications of hacker misuse. Also, theft of a user’s identity, bank information, and credit card details are potential consequences of such a scenario.

A second argument against Carnivore that is frequently cited among critics is the so-called ‘rogue agent problem’ (Eggen 2002a, b; Gugliotta and Krim 2001; O’Harrow 2001; Rosen 2002). Although yet to be substantiated in the case of Carnivore, critics of the software cite the potential for rogue agents to use the system for illegitimate espionage causes. Examples of instances of espionage by Special Agents include the recent case of Agent Robert Hannsen, who spied for the USSR, then Russia, for decades before being detected. Not only does espionage expose a vulnerability of the system, detection and prosecution of rogue agents will be nearly impossible.

A third argument against the Carnivore surveillance system is referred to as the 'mishap problem' (Eggen 2002a). Carnivore has the ability to disrupt internet service to all individuals on a particular ISP and to remove the control from that provider and place it in the hands of the FBI (StopCarnivoreNow 2003). The fear is that the software can thus virtually cripple internet service for possibly millions of individuals worldwide and as a result inflict substantial costs in terms of communication and e-commerce.

Finally, a discussion of the software's ethics necessitates consideration of its application. Because Carnivore is a relatively new tool and because the Justice Department has been closely guarded in revealing any information about the program, particularly that related to its targets, it is difficult to determine with any level of certainty how the software has been and will be utilized. A useful framework from which to hypothesize Carnivore's application is found in the theories of sociologist Black (1976, 1993). Black suggests that law itself is directly proportional to the social distance between two parties, so that the distance between adversaries in a given legal situation co-varies with legal development and application. Social distance can be understood in terms of differences regarding status characteristics such as race, ethnicity, and socioeconomic status. Previous legal action stemming from the U.S.A. Patriot Act – the extensive legislation that passed soon after 9/11, addressing numerous components of terrorism investigation and prevention – has seriously brought any equal application of related laws into question.

For example, there is the issue of 'enemy combatant' status. Yasser Esam Hamdi, an American born Arab, and John Walker Lindh, an American born Caucasian, were captured under identical circumstances on the Afghan battlefield shortly after September 11 (Jackman 2003). Both captives were deemed enemy combatants and brought to United States military bases as prisoners. However, Lindh was afforded his Sixth Amendment right to an attorney despite having fought against American troops. He was arraigned swiftly and publicly by the Justice Department. Those same rights, however, were denied to Hamdi, an ethnic minority who shared a similar background to the September 11 hijackers. Based on Black's social distance theory, the discrepancy in treatment between Lindh and Hamdi can be attributed, not to any of the facts of the case, but to the defendants' differences in ethnic background and related perceived sociopolitical and cultural threat.

Conclusion

In the totality of practices subsumed under the heading of the 'war on terror', FBI Project Carnivore makes up only a small fraction of an ever-increasing arsenal of governmental controls. Nonetheless, ethical or constitutional violations resulting from Carnivore may shape the future of our criminal justice system and tarnish its Constitutionally protected ideals because of the spread of highly intrusive systems of governmental control. Given the Justice Department's unwillingness to be forthcoming with information related to the use of Carnivore, it can only be hypothesized at this juncture what the consequences will be of the FBI's use of the software in the future. Specific information identifying the typical targets of the Carnivore system can at present not yet be ascertained, but in view of related legal actions stemming from the 'war on terror' it may be possible to predict the scope of monitoring in terms of the social distance among the parties involved.

With these observations in mind, it becomes questionable whether Project Carnivore will be implemented fairly. The social distance between the individuals involved in an investigation using Carnivore may instead serve as a key predictor of the software's use. Conjecture may be formed on the basis of examples such as the enemy combatant situation, the unequal application of the software, and allegations of alternative uses of Carnivore (e.g., censoring particular websites). All these issues will eventually need to be addressed by the Department of Justice. If the influence of social distance in the case of the prosecution of enemy combatants can serve as a guide, we may indeed expect what many already fear – that Project Carnivore will be improperly used to target only those who fit a certain profile.

Irrespective of the potential threat stemming from Project Carnivore, we have in this paper argued that the system in effect represents an increase in governmental control and a further diffusion of disciplinary power penetrating ever deeper into the community. Centrally oriented at locating and obtaining information, the Carnivore system has the potential to have chilling effects on free speech and thus contribute to produce, as Foucault (1977: 135–169) predicted, a nation of disciplined and docile bodies. The implications of a less than carefully controlled use of Carnivore can indeed be farreaching. The most likely scenario for actual Fourth-Amendment violations comes in the FBI's caveat of reserving the right to utilize Carnivore under 'emergency' situations.

Nowhere is the term emergency defined, and we are left to assume that it can be determined loosely at the discretion and perhaps whim of Justice Department officials.

A final concern is that in order to obtain a court order, the FBI would merely have to report to a federal judge that ordinary investigative techniques are not feasible – not that they have actually failed. Although there is probable cause attached to individuals under suspicion, federal law enforcement is not compelled to offer any probable cause that ordinary investigative techniques will not work. It may therefore be easier to obtain a court order for the use of Carnivore than official rhetoric would lead to suggest. Given the possibility of technical glitches in the software, also, law enforcement could feasibly access all information on an ISP, which would constitute a gross overreach of intent. Whatever the future holds for Carnivore, it is clear that its development and implementation signify a strengthening of and constitute one more building block towards the creation of a world monitored by an omnipresent social control.

Notes

1. To date, use of Carnivore has led to the removal of several websites, including: flagburningpage.com, azzam.com, iraradio.com, ogrish.com, freerepublic.com, allafrica.com, somalinet.com, raisethefist.com, yellowtimes.org, and palestine-info.Com/hamas.

References

- American Civil Liberties Union (2002). *Insatiable Appetite: The Government's Demand for New and Unnecessary Powers After September 11*. Washington, DC: Author.
- American Civil Liberties Union (2003). *The ACLU in the Courts Since 9/11*. Washington, DC: Author.
- Baddeley, S. (1997). Governmentality. In B.D. Loader (ed.), *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, pp. 64–96.
- Birdis, T. (2001). Justice Department asks Congress to clear wide-ranging antiterrorism legislation. *The Wall Street Journal* (September 19), A4.
- Black, D. (1976). *The Behavior of Law*. New York: Academic Press.
- Black, D. (1993). *The Social Structure of Right and Wrong*. New York: Academic Press.
- Cohen, S. (1985). *Visions of Social Control*. Cambridge: Polity Press.
- Collingwood, J.E. (2000a). *Editorial Responses, 24 July*. Available Online: www.fbi.gov
- Collingwood, J.E. (2000b). *Editorial Responses, 25 July*. Available Online: www.fbi.gov
- Collingwood, J.E. (2000c). *Editorial Responses, 7 August*. Available Online: www.fbi.gov

- Deflem, M. (1997). Surveillance and criminal statistics: Historical foundations of governmentality. In A. Sarat and S. Silbey (eds.), *Studies in Law, Politics and Society*, Vol. 17. Greenwich, CT: JAI Press, pp. 149–184.
- Deflem, M. (ed.) (2004). *Terrorism and Counter-Terrorism: Criminological Perspectives*. Sociology of Crime, Law, and Deviance, Vol. 5. Oxford, UK: Elsevier Science.
- Dunham, G.S. (2002). Carnivore, the FBI's e-mail surveillance system: Devouring criminals, not privacy. *Federal Communications Law Journal* 54, 543–566.
- Eggen, D. (2002a). Carnivore glitches blamed for FBI woes. *Washington Post* (May 29), A7.
- Eggen, D. (2002b). FBI misused wiretaps, according to memo. *Washington Post* (October 10), A14.
- Electronic Frontier Foundation (2000). "The Fourth Amendment and Carnivore." Statement of The Electronic Frontier Foundation Before the Subcommittee on the Constitution of the Committee on the Judiciary. United States House of Representatives, July 28, 2000. Available Online: www.eef.org
- Electronic Frontier Foundation (2003). "Chilling Effects of Anti-Terrorism". Available Online: www.eef.org
- Federal Bureau of Investigation (2000a). "Congressional Statement on Carnivore Diagnostic Tool, 7/24/00". Available online: www.fbi.gov
- Federal Bureau of Investigation (2000b). "Congressional Statement on Carnivore Diagnostic Tool, 9/6/00". Available online: www.fbi.gov
- Federal Bureau of Investigation (2003). "Carnivore Diagnostic Tool". Available online: www.fbi.gov
- Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.
- Foucault, M. (1980). *Power/Knowledge: Selected Interviews and Other Writings 1972–1977*. New York: Pantheon Books.
- Foucault, M. (1981). 'Omnes et Singulatim'. Towards a criticism of 'Political reason'. In S. M. McMurrin (ed.), *The Tanner Lectures on Human Values*, Vol. 2. Salt Lake City: University of Utah Press, pp. 223–254.
- Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon and P. Miller (eds.), *The Foucault Effect*. Chicago: University of Chicago Press, pp. 87–104.
- Garland, D. (1997). 'Governmentality' and the problem of crime: Foucault, criminology, sociology. *Theoretical Criminology* 1(2), 173–214.
- Gilman, J. (2001). Carnivore: The uneasy relationship between the Fourth Amendment and electronic surveillance of internet communications. *CommLaw Conspectus* 9, 111–129.
- Gooldstein, G. and Orr, C.H. (2003). Application of the U.S.A. Patriot Act to criminal investigations violates the First and Fourth Amendments. *Texas Bar Journal* 66(2), 40–52.
- Gordon, C. (1991). Governmental rationality: An introduction. In G. Burchell, C. Gordon and P. Miller (eds.), *The Foucault Effect*. Chicago: University of Chicago Press, pp. 1–51.
- Gugliotta, G. and Krim, J. (2001). Push for increased surveillance worries some. *Washington Post* (September 25), A4.
- Haas, T.C. (2001). Carnivore and the Fourth Amendment. *Connecticut Law Review* 34, 261–291.

- Holmes, P.K. (2001). FBI's Carnivore: Is the government eating away our right of privacy? *Roger Williams University Law Review* 7, 247–272.
- IIT Research Institute (2000). *Evaluation of Carnivore Diagnostic Tool*. Chicago: Author.
- Jackman, T. (2003). Judges uphold US detention of Hamdi. *Washington Post* (January 9), A1.
- Lerner, C.S. (2003). The reasonableness of probable cause. *Texas Law Review* 81(4), 951–1029.
- Marx, G.T. (1988). *Undercover: Police Surveillance in America*. Berkeley, CA: University of California Press.
- Marx, G.T. (1998). An ethics for the new surveillance. *The Information Society* 14(3), 171–185.
- Marx, G.T. (1999). Measuring everything that moves: The new surveillance at work. In I. Simpson and R. Simpson (eds.), *The Workplace and Deviance*. Research in the Sociology of Work, Vol. 8. Greenwich, CT: JAI, pp. 165–189.
- Marx, G.T. (2002). Technology and social control. In N. Smelser and P. Baltes (eds.), *International Encyclopedia of the Social and Behavioral Sciences*. Oxford, UK: Pergamon, pp. 15506–15511.
- Merl, S.R. (2001). Internet communication standards for the 21st century: International terrorism must force the U.S. to adopt 'Carnivore' and new electronic surveillance standards. *Brooklyn Journal of International Law* 27, 245–284.
- Merton, R.K. (1936). The unanticipated consequences of purposive social action. *American Sociological Review* 1(6), 894–904.
- O'Harrow, R. (2001). FBI's Carnivore might target wireless text. *Washington Post* (August 24), E1.
- Rosen, J. (2002). Liberty wins: So far Bush runs into checks and balances in demanding new powers. *Washington Post* (September 15), B1.
- Scheeres, J. (2001). "Suppression Stifles Some Sites". Available online: www.wired.com.
- Stanley, J. and Steinhardt, B. (2003). *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*. New York: ACLU.
- StopCarnivoreNow (2003). "The Backdoor, the Rogue Agent, and the Mishap: The Hidden Dangers of Carnivore". Available online: www.stopcarnivore.org
- Strauss, A.Y. (2002). A constitutional crisis in the digital age: Why the FBI's 'Carnivore' does not defy the Fourth Amendment. *Cardozo Arts and Entertainment Law Journal* 20, 231–258.
- Tountas, S. W. (2003). Carnivore: Is the regulation of wireless technology a legally viable option to curtail the growth of cybercrime? *Washington University Journal of Law and Policy* 11, 351–377.
- Tyson, J. (2003) "How Carnivore Works". Available online: www.howthingswork.com
- United States v. Katz (1967). 389 U.S. 347.
- Vlahos, KB. (2001). "FBI Seeking to Wiretap Internet". Available online: www.foxnews.com
- Voors, M.P. (2003). Encryption regulation in the wake of September 11, 2001: Must we protect national security at the expense of the economy? *Federal Communications Law Journal* 55(22), 331–350.
- Walters, R. (2003). New modes of governance and the commodification of criminological knowledge. *Social and Legal Studies* 12(1), 5–26.