Policing the abstract: Some observations on policing cyberspace

Laura J. Huey
University of British Columbia
Vancouver, B.C.

L'espace cybernétique constitue un endroit difficile à surveiller. L'auteure affirme que les défis à relever sont surtout abstraits et découlent des habitudes des policiers; c.-à-d., le milieu policière est fondé sur des perceptions de la fonction policière qui s'exercerait surtout dans des espaces géographiques/physiques. Par contre, le cyberspace est perçu comme étant fondamentalement différent et abstrait, là où les actions policières normales ne sont pas facilement applicables. L'auteure soutient que cette apparente incompatibilité explique en partie le peu d'enthousiasme des organismes policiers à enquêter sur les crimes commis dans l'espace virtuel.

Cyberspace continues to pose significant challenges to policing. The paper's author argues that some of the problems raised are conceptual in nature and stem from habitus: that the police culture is grounded in a perceptual schema tied to understandings of the policing function as being linked primarily to physical/geographical notions of what constitutes territory to be policed. Cyberspace, by contrast, is seen as being fundamentally different or abstract, and thus not a space where normal policing strategies are easily applied. It is suggested that this perceived incompatibility offers a partial explanation for the unwillingness of many local policing agencies to investigate online crimes.

Introduction

With the emergence of complex systems of computer technologies and data networks, there has been a renewed desire to understand, to delineate, and to articulate the interdependent relations of the physical to the social and vice versa. Among other results, this has led to the development of a rather overblown claim that cyberspace represents a new, entirely unique entity – an abstract form of the social. This new entity is
perceived to be devoid of links to traditional understandings of what constitutes the physical. Instead of viewing computers as physical phenomena, somehow, for many, they come to represent magic boxes that mysteriously obey commands upon direction. Much of the blame for this misconception can be attributed to a lack of understanding of the nature of computers and telecommunications technology.

What I would like to suggest here is that the magic box perception of computer technology may offer another explanation for the reluctance of many local police agencies to tackling online crimes (Groover 1996; Goodman 1997; Charney in Suydam 1999; Duncan 1999; Hyde 2000a). Other authors have cited as causes, lack of interest (Hyde 2000b), lack of funds or resources (Goodman 1997; Hyde 2000b), lack of public outcry over online crimes (Goodman 1997), and lack of training (Davis 1998). These are all legitimate explanations; however, I am most inclined to agree that lack of training and basic understanding is a fundamental problem. Therefore, I offer a slightly different, although complementary explanation. What I wish to suggest is that not only is the police institution not immune from the magic box view of the new technology, but rather that it is particularly susceptible to it. This is because historically the nature of policing in society has been intricately tied to spatial arrangements. The public police meet their prescribed mandate through techniques involving the oversight of carefully defined physical territories. These physical territories are defined in a multitude of ways, including the separation between public and private domains, police jurisdictions, the creation of specific service zones within jurisdictions, and so on. By examining how territory is understood by the police, we see how difficulties result when attempts are made to apply a physically grounded conception of territory to cyberspace—which is perceived as being different (i.e., non-physical).

In the sections that follow, I briefly discuss the relationship of police to territory. Then I examine some of the writings of police authors[1] on the subject of cyber-policing and, in particular, the problems that they suggest that cyberspace presents for police. This analysis leads me to conclude that many arguments that present cyberspace as being inherently problematic for public policing are not fully supported. The
benefit of this analysis is that it provides a means for combating some of the reluctance of local agencies to respond to online crimes.

The policing of territory

There are a variety of ways in which both the culture of policing, and the requirements of the job itself, come to instill and reinforce spatial/geographical perceptions of the police function. From the very beginning of their careers, officers are assigned to divisional districts, sent out to cover territory through patrol work, and are assigned means or methods of conducting patrol that are most appropriate to the space they work in (such as squad cars, bicycles, horse, foot). In discussing the policing of inner cities, McCormick and Visano (1992: 236) note that “the police typically occupy long periods of their shifts concerned with activities on the street in order to control public space... judgments are made regarding the visibility, accessibility and stability of neighbourhoods.” Police officers come to understand, and perhaps to identify with the neighbourhoods that they patrol, to ‘get a feel for’ the space.

In *Policing the Risk Society*, Ericson and Haggerty (1997) document a myriad of other ways in which physical space and spatial arrangements come to dominate the discourse of policing – increasingly, due to reliance on technical policing solutions. To illustrate, they note that many police organizations within Canada have purchased computerized mapping systems that “allow territories to be broken down into ever smaller units” (Ericson and Haggerty 1997: 137). We are advised that, “equipped with this technology, the patrol officer can obtain detailed knowledge of officially recorded crimes and other problems that have occurred in narrowly defined zones within a patrol area – blocks, buildings, and even parts of buildings”. As one officer interviewed in Ericson and Haggerty’s (1997:137) study suggests, “You can see where this would be a big help to the community police officer ... He could get a geographic feel for the location of prostitution or sexual assault cases for a specific period if he wanted them” (italics mine). Police video surveillance cameras function not only panoptically as electronic eyes and ears (Lyon 1994), but also assist police in “[tracing] risks to territories” (Ericson and Haggerty 1997: 137). The information produced
from these technologies directs not only the individual officer in
terms of shaping her or his response to events within target areas,
but is also used to shape the various institutional policies towards
those same geographic entities and the individuals occupying
them.

Examining cyberspace as ‘different’ arguments

Where a culture is locked into a worldview, it may be seen to
create frustration when there is an inability to effect a simple
transposition of one system or perceptual scheme to what appears
to be another. This frustration is clearly evident in the writings
of police authors who discuss the unwillingness of police agencies
to adopt online policing (Goodman 1997; Hyde 2000a; 2000b).

Unlike those who argue, implicitly or explicitly, that
cyberspace forces the police and other co-ordinate state systems
to engage in a re-conceptualization of ‘territory’ in order to
accommodate more abstract notions of space, I suggest that this
is not the case for two reasons. First, cyberspace is physical.
Second, cyberspace is analogous, and in many ways a good
simulation. While it remains an imperfect, inexact copy of the
real world, where the fit is imperfect, the analogous nature of
cyberspace requires no radical shift\(^2\) in how the police
understand their function. I will demonstrate both of these points
throughout the remaining discussion.

The ‘non-physical’ or ‘ether’ problem

In relation to the abstract nature of cyberspace, it is frequently
perceived as being ‘different’ because, even though computers
and network components reside in physical bodies of metal and
wire, they are nonetheless believed to be unlike ‘ordinary’ physical
objects that can be seen, touched, experienced directly. Davis
(1998: 51) makes this point when he notes that “most of us grew
up in an environment where information was gleaned from the
press, the education system, libraries and other places of learning
– all physically tangible. But the Internet has meant that, in a
policing sense, evidence of crime has to be acquired from what
people see or where information has been recorded in some way.”

Another example of how this perceived abstract nature creates
difficulties is illustrated by comments made by Wall (1998). In
discussing problems related to policing cyberspace. Wall (1998) states that the Internet facilitates criminal activity in two ways. First, it serves as a vehicle for existing activities. Second, because "it has created an environment, a cyberspace, which has facilitated the creation of entirely new types of activities which are largely free of traditional and terrestrial constraints". In relation to Wall's second point, there are two particular misconceptions present that I would like to tackle. First, this notion that cyberspace activities are "free of traditional and terrestrial constraints" is a fiction; computer data is not akin to ether. All computer and network activities are spatial and temporal phenomena in that they necessarily involve that data exist, even temporarily, on a physical device at some location, at some point in time. For example, data exists physically on hard drives, on diskettes, on tapes, on the cylinders of direct access storage devices (DASD), on paper, in the jottings and scribblings of users and creators, and as electronic impulses travelling across wires.

Indeed, some could argue that with 'data taps'[^3], and the variety of ways in which electronic data can be stored, investigators have more, rather than fewer, opportunities to investigate computer-related crimes successfully. In many cases, evidence of criminal activities on the Internet is both easy to discover and to obtain as most Internet Service Providers, webmasters, and so on, regularly perform back ups of data, which can be obtained by the police through search warrants. In Canada, warrants may be obtained under s. 487 of the Criminal Code, with no special burden, beyond setting out the requisite particulars of place, time, and items to be searched/seized placed upon the police in terms of how a warrant to search or seize a computer or data is to be drafted or executed.

Online chat rooms are perhaps slightly more problematic in terms of gathering data, as chat room owners do not always monitor and back up chat data. Users of chat room facilities run the risk of encountering online witnesses to their activities. Furthermore, the relative anonymity of the cyberspace provides police with a covert means of gathering evidence of criminal activity that many not be otherwise available. For example, in the case of R. v. Hurtubise and Hurtubise (1997), an unreported decision of the Supreme Court of B.C. (New West.), a police officer
set up an account on a local Bulletin Board System (BBS) using an alias, and then repeatedly accessed child pornography, which he downloaded as evidence onto his computer. The defendants were convicted of distributing child pornography under s. 163 of the Criminal Code and, although they later appealed, they did not cite the officer's ruse as a ground of appeal under s.8 (the search and seizure provisions) of the Charter. Had the appellants raised this issue as a ground of appeal, it is doubtful whether they would have been successful given a similar case involving offences under the Canadian Copyright Act, R.S.C. 1985, c. C-42. In R. v. Morin, [1996] R.J.Q. 1758 (Crim. Ct.), a police officer recorded the contents of communications with a BBS operator that were later used to obtain a search warrant. The defendant tried to have the communications and the evidence from the warrant excluded on the grounds that the officer's actions constituted participant surveillance (in R. v. Duarte (1990), [1990] 1 S.C.R. 30, the Supreme Court of Canada held that the surreptitious use of electronic surveillance by police or informers constitutes an unreasonable search and seizure under the Charter). The Court, in Morin, however, held that the BBS operator had had no reasonable expectation of privacy in the content of his messages given that the recording of electronic communications (such as e-mail) is standard practise, and that, in fact, the accused had sent out general invitations to communicate with him on more than one occasion. Therefore, it was open to anyone, including the police, to respond (R. v. Morin).

The second problem I note with Wall's analysis is his claim that cyberspace lends itself to the creation of new crimes. While it is certainly the case that computer technology has spawned new methods for committing crime (such as computer viruses or credit/debit card frauds), as well as new means of communicating criminal activity (underground chat rooms and BBS's), the activities, in and of themselves, are mere variants of existing crimes. Thus, they are not entirely outside the scope of traditional understandings of what constitutes the offences of vandalism (viruses), fraud (credit/debit schemes), conspiracy (communicating in an underground chat room for the purpose of committing a crime), and conversion of property (theft of CPU cycles on another's machine). This also holds true for 'newer' crimes that Wall identifies, such as intellectual property theft and economic espionage. Again, these crimes that Wall correctly
suggests are largely tortious in nature rather than criminal offences[6], pre-date the Internet. Companies have spied on each other, and attempted to gain access to others' trade secrets for much longer than the Internet has been in existence. The Internet's role in this process has largely been to provide a new means by which an old activity can occur.

The 'global' problem

The issue of police agents' attempts to transpose their conception of territory onto cyberspace also arises in relation to discussions as to the complicated nature of policing a global system that has no respect for police jurisdictions. Indeed, the notion that public policing in cyberspace faces immense challenges because of the Internet's global scope is a predominant theme in much of the literature (Duncan 1999; Goodman 1997; Davis 1998). In particular, to borrow from Latour (1993: 177), the challenge is seen to lie in the fact that a global network "remains local at all points." Thus, issues such as determining the jurisdiction of an offence – a simple network transaction – are perceived to be inordinately complex because such efforts may require extensive cooperation from authorities at each of the local points necessarily involved. Such cooperation may be local, regional, national, and international, thus compounding the difficulty.

Both Goodman (1997) and Davis (1998) pose hypothetical scenarios intended to demonstrate the problems of pursuing cyberspace cases across law enforcement boundaries. The difficulties that each of these authors raise are not slight, particularly with respect to the issue of obtaining search warrants in foreign jurisdictions due to local computer privacy laws, and the ability of the Internet to increase, with its speed and reach, the number and scope of crimes perpetrated across jurisdictions. These problems are not, however, insurmountable, as an increasing number of countries maintain federal agencies that have the expertise in both computer and transnational crime to take on such cases or to provide support to local agencies. In the United States, the F.B.I. maintains offices in both Washington and in the Silicon Valley in order to provide such assistance, whereas in Canada local jurisdictions can benefit from the services of the Technical Division of the RCMP. Furthermore, in
some instances it is the international nature of the crime that lends itself to detection. For example, in *R. v. Daniels* (1999) 177 D.L.R. (4th) 599, the activities of the accused were detected as a result of an investigation by U.S. Customs officials into a Mexican bulletin board that was distributing child pornography. U.S. officials contacted the R.C.M.P. after the accused's name turned up on a list of subscribers to the service.

Aside from the exceptions noted, both authors cited fail to distinguish further how investigations involving network transactions differ from more traditional crimes that similarly span jurisdictions. For example, in organized crime cases involving multiple countries, obtaining evidence of such activities may necessitate securing cooperation from other agencies in relation to obtaining search warrants, extradition orders, and so on. The procedures for doing so are often the same as those involved in tracing and prosecuting a computer hacker (again, excluding any local laws with respect to computer privacy). This is not to suggest, however, that such obstacles are not important considerations for the police, only that cyber-crimes can again be seen as analogous to other forms of traditional crime.

**The 'ultra-social' problem**

While I have been stressing the geographical nature of policing, the police also operate at the level of the social. Again, their perception as shaped by *habitus* may sometimes bar them from seeing their role as operating outside of geographical space. This can be seen in discussions of cyber-policing and the false fear of cyberspace as an amplified form of the social. In the almost singular focus on cyberspace as hyper-reality, what is missing from many analyses is acknowledgement that cyberspace is not simulacra. While it is an imperfect copy of the world, its spaces do mirror existing social realities by duplicating oppression and resistance, by utilizing conventional forms of social exchange (or near-variants), and by permitting the dissemination of techniques of normalization. Because cyberspace has also frequently been promoted as 'different' in the sense of being 'ultra social' or 'hyper-social', some police agents perceive it as requiring them to learn to operate in a way that is fundamentally different from their ordinary means of
effecting order. Davis (1998: 54) clearly advances this position: “The Internet and its many different systems have created an environment which is in many ways unique. The communities that inhabit the Internet are truly global but at the same time local. The behaviour and language is different and therefore it demands from a criminal investigator a whole new skills and abilities profile.”

Davis' comment suggests two things. First, that 'terrestrial' policing is not perceived by the police as being particularly social because it is local, and thus consists of behaviour and language already understood by the police – a strange, unlikely position to advance. And/or, that cyberspace is ultra-social because it is global and thus demands new modes of thinking and communicating.

Regardless, what Davis (1998) and others who share this view miss is that policing is, of necessity, already ultra-social. Indeed, traditional policing is perhaps best thought of as geo-social. With today's ethnically diverse populations, police officers must daily negotiate different languages and cultures in order to perform their duties. And, while computers do demand that users utilize a different language from regular English, French, Spanish and so on, in order to communicate, computers duplicate natural language in that they similarly follow syntax and logic rules. There is also an increasing use of symbols (emoticons) and graphical user interfaces (the Windows desktop) that are more easily understood by users.

Final thoughts

Despite claims that the character of police work is changing (Manning 1992), it is apparent that the traditional geographically rooted perceptual set that the police apply to their work has adapted little. Indeed, the failure of many local agencies in North America to come to grips with the Internet illuminates this problem clearly (Duncan 1999). Some might suggest that given the perceived difficulty of attempting to modify the habitus in which this perceptual set is created and reinforced, that it is simply easier to leave cyberspace to regulate itself. As Goodman (1997) notes, others may question whether, because of the lack
of sustained public outcry over computer crimes in comparison to 'street crimes', that computer crime should even be a concern of public policing.

In response to those who perceive cyber-policing as being a task fraught with immense difficulties, I would suggest that this is not the case. While other serious impediments still remain, and clearly need to be addressed, there is nothing inherently problematic about online policing that should bar local agencies from adopting Internet policing programs. Indeed, basic education about the nature of computers and telecommunications technology would easily resolve any lingering doubts on this score.

In short, as Hyde (2000a) suggests, "...the Internet is a free and accessible entity where normal policing systems can be applied". The culture of policing could, as Hyde (2000b) similarly notes, take advantage of the opportunities that this technology has to offer it.

Notes

1. The police authors whose writings were examined here include: Duncan (1999), a Corporal in the Technological Crime Section of the RCMP; Hydc (2000a, 2000b), Chief Superintendent of the West Yorkshire Police; Goodman (1997), a Senior Sergeant/Investigator with the Los Angeles Police Department; Groover (1996), a volunteer deputy sheriff with the Hanover County, Virginia, Sheriff's Department; and Davis (1998), who is a Internet investigator with the West Midlands fraud squad. Because so few articles have been published on the subject of cyber-policing, I have also included an article by David Wall (1998), who is a Senior Lecturer in Criminal Justice at the University of Leeds, and a Deputy Director of the Centre for Criminal Justice studies. Wall is a well-known researcher in the areas of policing, cyber law, and cybercrimes. Please note that the occupations and titles listed are current as of the publication date.

2. While I suggest that no 'radical shift' is necessary, for many countries there remains a need for some minor re-working of laws, policies, and practises.

3. A "data tap" is a device placed on a network that can 'eavesdrop' on traffic on that network, including email and other transmissions.

4. In Canada, the theft of computer-related services is an offence under section 342.1 of the Criminal Code.
5. Personal communication.

6. Personal communication.

References

Davis, David J.

Duncan, Michael

Ericson, Richard V. and Kevin D. Haggerty

Goodman, Marc D.

Groover, Richard S.

Hyde, Stuart

Hyde, Stuart

Latour, Bruno

Lyon, David

Manning, P.K.

McCormick, Kevin R.E., and Livy A. Visano


Suydam, Margot

Wall, David S.