



## Chapter 12

---

# Afterword: technopolice

*Stéphane Leman-Langlois*

Technology has always been a central element in warfare. The army with the best equipped soldiers, all other things being equal, had an edge over enemies less technologically advanced. This applies to weapon and defence systems, of course, but also to support equipment, to information systems and to the logistics line needed to move, distribute and maintain the battle technologies.

The war on crime, no longer a metaphor – like the war on poverty or the war on cancer – also shares this preoccupation with the enemy's capabilities and with the question of whether 'ours' will provide the clear, lasting superiority we seek. Sometimes this preoccupation comes from a rather straightforward contrast between the technologies used by criminals and the technologies available to police. For instance, it is easy to compare the firepower of criminal gangs with that of police, or the abilities of Internet paedophiles with those of the cybercops who chase them. However, one must bear in mind that, while the police adoption of technology is quite a deliberate, organized, often debated, delayed, mediatized, etc., process, those who engage in criminal, forbidden or otherwise irritating behaviour with the help of technology are in a much more spontaneous, opportunistic and 'natural' dynamic. Today's credit card skimmer is not yesterday's mugger. Criminals do not adopt new technologies; they do not modify their trade. New criminals are seduced by the opportunities offered by the new technologies that suffuse their world – just like technopolice advocates and practitioners.

At other times the contrast in technology mobilization is more indirect: in a recent Royal Canadian Mounted Police (RCMP

experiment to use the spectrographic analysis of satellite images to detect marijuana plants, one technology (the peppering of small clutches of marijuana plants in the middle of large cornfields) won over the other (the insufficient 4 m resolution of the imaging satellite available to police) (CCRP 2002).

Finally, in many instances police technology is contrasted not to the technologies or tactics employed by criminals but to a type of crime, or sometimes to 'crime' in general. The involved technologies are guaranteed to impact significant aspects of criminality and to improve the general security of citizens. Video cameras are among such technologies. Their connection with their objective is a pure abstraction, based on symbols (that which is hidden must be revealed), theories (surveillance deters) or faith (technology *works*; it will work here as well).

For all these reasons, we can conclude that technocrime and technopolicing are not geometric opposites, mirror images; in fact, the two sets of representations merely overlap in some technologically minor, yet sociologically highly significant aspects. Technopolicing is not simply an answer to a growing or increasingly dangerous body of technocrimes. Technocrime is not the only response crooks can make to the better policing of their previous, low-tech activities. Technocrime is, of course, a spectre raised by politicians, civil servants or industrial entities to justify more technopolicing, but it is not limited to that.

What we can say about the relationship of technocrime to private, public and hybrid forms of technopolicing is as follows:

1. They both have objective and constructed aspects. As is the case with conventional forms of crime, crooks, swindlers and abusers online and off are absolutely convinced that their actions do not create 'true' victims, especially when insurance, credit-card policy or bank practices end up mitigating the negative effects of their exploits on their victims. From the policing point of view, some technologies benefit from what might be described as axiomatic effectiveness. Their ability to fulfil their objectives is, in a way, built into their very definition. Such is the case of surveillance cameras. Like homeopathy and acupuncture, these technologies are evaluation-proof: no amount of negative findings will affect their image, and placebo-level positive findings will always be available.

2. The constructed aspects always trump the objective. Police administrators and politicians are more likely to use the technology discourse in what Edelman would call a hortatory effort to reassure

and to appear in control, and police officers on the ground are more likely to feel sceptical about high-tech approaches to crime-solving. As Manning shows in Chapter 11, street-level police intervention remains decidedly low tech. Brodeur (Chapter 9) demonstrates that the equivalent phenomenon dominates in police investigations, and Lemieux (Chapter 8) in the realm of criminal intelligence outfits. Yet police objectives, budgets, organizational structure, tactics and strategies are decided elsewhere.

3. At the same time, Lyon (Chapter 10) shows how the 'freeloader' government discourse pushes the policing of social entitlements into increasingly intense generalized surveillance. Whether or not first-line government agents (as well as private enterprises) actually apply the new surveillance technologies the politicians bought in precisely the intended way, they *will* use them. Regardless of the adaptations, incompetence, system failures and other shortcomings pointed out by Manning, the new tools will find new users.

4. They are constructed both by individuals and groups who are engaged in either form of activity, as well as by individuals who are not. Our perceptions of various technocrimes are the result of massive quantities of discourse coming from all directions; cybercrime is an especially good illustration of this phenomenon. Between commercial, government, institutional, police, military, media and expert constant *talk* about cybercrime, we are bombarded with various versions of exotic threats to our jobs, families, savings, water supply, etc. (The most exotic is that of Second Life miscreants who prey on other virtual visitors, as described in Chapter 6 by Whitson and Doyle.) These claims are often contradictory, as is apparent in the chapters by Nhan and Huey (Chapter 5) and Gagnon (Chapter 4), as they are contingent on particular social and economic factors unique to each claim-maker.

5. Private industry remains ahead of the public police. In a way, that developmental differential is easy to explain, since most technologies (civilian and military) are developed by the private sector. While low-tech, traditional forms of policing were closely enmeshed with legal and political demands, expedients and operational frameworks, technopolicing hinges on the decisions, discoveries and market strategies of private enterprise. Today this is most apparent in the aggressive marketing/lobbying of Taser International for the acceptance of its products, for instance.

6. As Brin (Chapter 2) describes our transparent future, many will find little comfort in the idea that individual spying cancels out, or makes up for, personal info- or techno-nakedness. Either way, the



## Technocrime

tide is indeed in and on the way up, and no amount of legislation, contestation or retreat is likely to stem it or even slow it down. One may not like Brin's version of bending in the wind, but flexibility is going to be the answer. Already, such flexibility can be seen in the rapid redefinition of 'privacy' that is taking place, as described in my Chapter 7. We may not *like* the new privacy, but it is there and offers a number of possible keys to our feeling safe in the next society.

In the 'information society,' technology occupies a central position. Not only is it concretely at the centre of many of our activities, but it also symbolizes the essence of what is still 'modern' in our late-modern culture: the belief that we can voluntarily ameliorate our human condition. Though it also stands for what is wrong with us – pollution, unsafe foods, Beck's nuclear risks – for most of us, technology, whether medical, information, entertainment, transportation or other, embodies the better future. Technocrime, as a perversion of this promise or at least an irritant side-effect comparable with pollution, must always be accompanied by technopolicing and its objective, technosecurity.

## Reference

Canadian Police Research Centre (CCRP (2002) *Operation SABOT and Illicit Crop Information Management Using Satellite Imagery*. Richmond, BC: RADARSAT International.